



where solutions begin



I-Fly Wireless Broadband Router

User's Manual (v1.0)

COPYRIGHT

The Atlantis Land logo is a registered trademark of Atlantis Land SpA. All other names mentioned may be trademarks or registered trademarks of their respective owners. Subject to change without notice. No liability for technical errors and/or omissions. Copyright © 2002 by this company.

DISCLAIMER

This company makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

FCC Warning

This equipment has been tested and found to comply with the regulations for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this user's guide, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Important Note

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. The antenna(s) used for this equipment must be installed to provide a separation distance of at least 30 cm from all persons.

This equipment must not be operated in conjunction with any other antenna.

INDEX

CHAPTER 1	1
1.1 AN OVERVIEW OF THE I-FLY WIRELESS BROADBAND ROUTER	1
1.2 PACKAGE CONTENTS	2
1.3 I-FLY WIRELESS BROADBAND ROUTER FEATURES.....	2
1.4 SYSTEM REQUIREMENTS	3
1.5 I-FLY WIRELESS BROADBAND ROUTER APPLICATION.....	3
CHAPTER 2	5
2.1 CAUTIONS FOR USING THE I-FLY WIRELESS BROADBAND ROUTER	5
2.2 THE FRONT LEDS	5
2.3 THE REAR PORTS	6
2.4 CABLING	6
CHAPTER 3	7
3.1 BEFORE CONFIGURATION	7
3.2 CONNECTING THE I-FLY WIRELESS BROADBAND ROUTER	7
3.3 CONFIGURING PC IN WINDOWS	8
3.3.1 For Windows 95/98/ME.....	8
3.3.2 For Windows NT4.0.....	10
3.3.3 For Windows 2000.....	11
3.3.4 For Windows XP	13
3.4 TEST TCP/IP.....	15
3.5 CONFIGURING INTERNET EXPLORER	15
3.6 FACTORY DEFAULT SETTINGS	16
3.6.1 LAN and WAN Port Addresses	16
3.7 RESET	16
3.8 CONFIGURAZIONE DEL ROUTER TRAMITE BROWSER.....	17
3.8.1 LAN Settings.....	18
3.8.1.1 LAN&DHCP Server	18
3.8.1.2 WAN	19
3.8.1.3 Password	21
3.8.1.4 Time	22
3.8.1.5 Dynamic DNS	22
3.8.2 Wireless.....	22
3.8.2.1 Basic.....	22
3.8.2.2 Authentication.....	23
3.8.2.3 Advanced	24
3.2.3.4 802.1x.....	24
3.8.3 STATUS.....	25
3.8.3.1 Device Information	25
3.8.3.2 Log	26
3.8.3.3 Log Setting.....	27
3.8.3.4 Statistics	28
3.8.3.5 Wireless.....	28
3.8.4 ROUTING	28
3.8.4.1 Static	28
3.8.4.2 Dynamic	29

3.8.4.3 Routing Table.....	30
3.8.5 Access.....	30
3.8.5.1 Filter.....	30
3.8.5.2 Virtual Server.....	34
3.8.5.3 Special AP.....	37
3.8.5.4 DMZ.....	38
3.8.5.5 Firewall Rule.....	38
3.8.6 Management.....	39
3.8.6.1 SNMP.....	39
3.8.6.2 Remote Management	39
3.8.7 Tools.....	40
3.8.7.1 Restart	40
3.8.7.2 Settings.....	40
3.8.7.3 Firmware	41
3.8.7.4 Ping Test	41

APPENDIX A 42

 QUICK SETUP WITH WIZARD..... 42

APPENDIX B 49

 TECHNICAL FEATURES..... 49

APPENDIX C 51

 GLOSSARY..... 51

APPENDIX D 55

 SUPPORT..... 55

Chapter 1

Introduction

And' besides available on CDRom a Quick Start Guide for a fast configuration.

1.1 An Overview of the I-Fly Wireless Broadband Router

The device for a total freedom of movement without losing the connection. Easy to be installed and fast and flexible, with I-Fly Wireless Broadband Router there is no more obligation for a fixed working place: you can easily work or navigate for fun from your own garden or in different rooms of your office, always in wireless connection.

I-Fly Wireless Router is extremely flexible and you can choose the technology for your connection to internet, i.e. through an ISDN device or through the fast solution of the broadband. Your whole office can be connected to the web simultaneously and throughout, thanks to our I-Fly Wireless Router, which can serve up to 253 users. The Roaming function gives you a complete freedom of movement and two or more Wireless Router can serve wireless also large headquarters.

Thanks to advanced security functions which are integrated and thanks to the throughput of the protocol IEEE802.11G you are going to have a fast and flexible wireless net, hacker safe.

The chipsets fully support Wi-Fi Protected Access (WPA) and the IEEE 802.11i draft security standards in hardware and high-speed encryption engines for both the Temporal Key Integrity Protocol (TKIP) and the Advanced Encryption Standard (AES) with no performance degradation.

Last, but not least, this product implements Atheros Super G™ (available for devices with chipset Atheros) capabilities to deliver 108 Mbps raw data rates and 90 Mbps TCP/IP throughput for 802.11g wireless LANs (Real-time hardware data compression, Dynamic transmit and modulation optimization and Standards-compliant bursting mode adapts to the network).

This product also serves as an Internet firewall, protecting your network from being accessed by outside users. Not only provides the natural firewall function (Network Address Translation, NAT), it also provides rich firewall features to secure a user's network. All incoming data packets are monitored and filtered. Besides, it can also be configured to block internal users from accessing to the Internet.

The product provides three levels of security support. First, it masks LAN users' IP addresses which are invisible to outside users on the Internet, making it much more difficult for a hacker to target a machine on your network. Secondly it can block and redirect certain ports to limit the services that outside users can access. For example, to ensure that games and other Internet applications will run properly, a user can open some specific ports for outside users to access internal services in the network. Finally it can also detect and block many Hacker Patterns and not allow hackers into your network.

Integrated DHCP services, client and server, allows up to 253 users to get their IP addresses automatically on boot up from the product. Simply set local machines as a DHCP client to accept a dynamically assigned IP address from DHCP server and reboot. Each time a local machine is powered up; the router will recognize it and assign an IP address to instantly connect it to the LAN.

For advanced users, The Virtual Server function allows the product to provide limited visibility to local machines with specific services for outside users. An ISP provided IP address can be set to the

product and then specific services can be rerouted to specific computers on the local network. For instance, a dedicated web server can be connected to the Internet via the product and then incoming requests for HTML that are received by the product can be rerouted to the dedicated local web server, even though the server now has a different IP address. In this example, the product is on the Internet and vulnerable to attacks, but the server is protected.

Virtual Server can also be used to re-task services to multiple servers. For instance, the product can be set to allow separated FTP, Web, and Multiplayer game servers to share the same Internet-visible IP address while still protecting the servers and LAN users from hackers.

1.2 Package Contents

1. One I-Fly Wireless Broadband Router
2. One CD-ROM containing the online manual
3. One Quick Start Guide
4. One CAT-5 LAN cable
5. One AC-DC power adapter (5V DC, 2A)
6. Warranty

If any of the above items are missing, please contact your reseller.

1.3 I-Fly Wireless Broadband Router Features

I-Fly Wireless Broadband Router provides the following features:

- **Interoperable with IEEE802.11g and IEEE802.11b**
- **Atheros Super G™ capabilities to deliver 108 Mbps** raw data rates and 90 Mbps TCP/IP throughput for 802.11g wireless LANs (Real-time hardware data compression, Dynamic transmit and modulation optimization and Standards-compliant bursting mode adapts to the network)
- **WPA (with PSK, TKIP):** The chipsets fully support Wi-Fi Protected Access (WPA) and the IEEE 802.11i draft security standards in hardware and high-speed encryption engines for both the Temporal Key Integrity Protocol (TKIP) and the Advanced Encryption Standard (AES) with no performance degradation.
- **Fast Ethernet Switch:** A 4-port 10/100Mbps fast Ethernet switch is supported in the LAN site and automatic switching between MDI and MDI-X for 10Base-T and 100Base-TX ports is supported. An Ethernet straight or cross-over cable can be used directly, this fast Ethernet switch will detect it automatically.
- **Dual antenna:** Dipole External removable Antenna (SMA) and Embedded Antenna
- **Quick Installation Wizard:** Supports a WEB GUI page to install this device quickly. With this wizard, an end user can enter the information easily which they from the ISP, then surf the Internet immediately.
- **Universal Plug and Play (UPnP) and UPnP NAT Traversal:** This protocol is used to enable simple and robust connectivity among stand-alone devices and PCs from many different vendors. It makes network simple and affordable for users. UPnP architecture leverages TCP/IP and the Web to enable seamless proximity networking in addition to control and data transfer among networked devices.
- **Network Address Translation (NAT):** Allows multi-users to access outside resource such as Internet simultaneously with one IP address/one Internet access account. Besides, many

application layer gateway (ALG) are supported such as web browser, ICQ, FTP, Telnet, E-mail, News, Net2phone, Ping, NetMeeting and others.

- **Firewall:** Supports SOHO firewall with NAT technology. Automatically detects and blocks the Denial of Service (DoS) attack. The URL-blocking, packet filtering and SPI are also supported. The hacker's attack will be recorded associated with timestamp in the security logging area. More firewall features will be added continually, please visit our web site to download latest firmware.
- **Dynamic Domain Name System (DDNS):** The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname. This dynamic IP address is the WAN IP address.
- **PPP over Ethernet (PPPoE):** Provide embedded PPPoE client function to establish a connection. Users can get greater access speed without changing the operation concept, sharing the same ISP account and paying for one access account. No PPPoE client software is required for the local computer. The Always ON, Dial On Demand and auto disconnection (Idle Timer) functions are provided too.
- **Virtual Server:** Users can specify some services to be visible from outside users. The router can detect incoming service request and forward it to the specific local computer to handle it. For example, users can assign a PC in a LAN acting as a WEB server inside and expose it to the outside network. Outside users can browse an inside web server directly while it is protected by NAT. A **DMZ** host setting is also provided to a local computer exposed to the outside network, Internet.
- **Rich Packet Filtering:** Not only filters the packet based on IP address, but also based on Port numbers. It also provides a higher-level security control.
- **Dynamic Host Control Protocol (DHCP) client and server:** In the WAN site, the DHCP client can get an IP address from the Internet Server Provider (ISP) automatically. In the LAN site, the DHCP server can allocate up to 253 client IP addresses and distribute them including IP address, subnet mask as well as DNS IP address to local computers. It provides an easy way to manage the local IP network.
- **Static and RIP1/2 Routing:** Supports an easy static table or RIP1/2 routing protocol to support routing capability.
- **SNTP:** An easy way to get the network real time information from an SNTP server.
- **Web based GUI:** supports web based GUI for configuration and management. It is user-friendly with an on-line help, providing necessary information and assist user timing. It also supports remote management capability for remote users to configure and manage this product.
- **Firmware Upgradeable:** the device can be upgraded to the latest firmware through the WEB based GUI.
- **Rich management interfaces:** Supports flexible management interfaces with local console port, LAN port, and WAN port. Users can use terminal application through console port to configure and manage the device, or Telnet, WEB GUI, and SNMP through LAN or WAN ports to configure and manage a device.

1.4 System Requirements

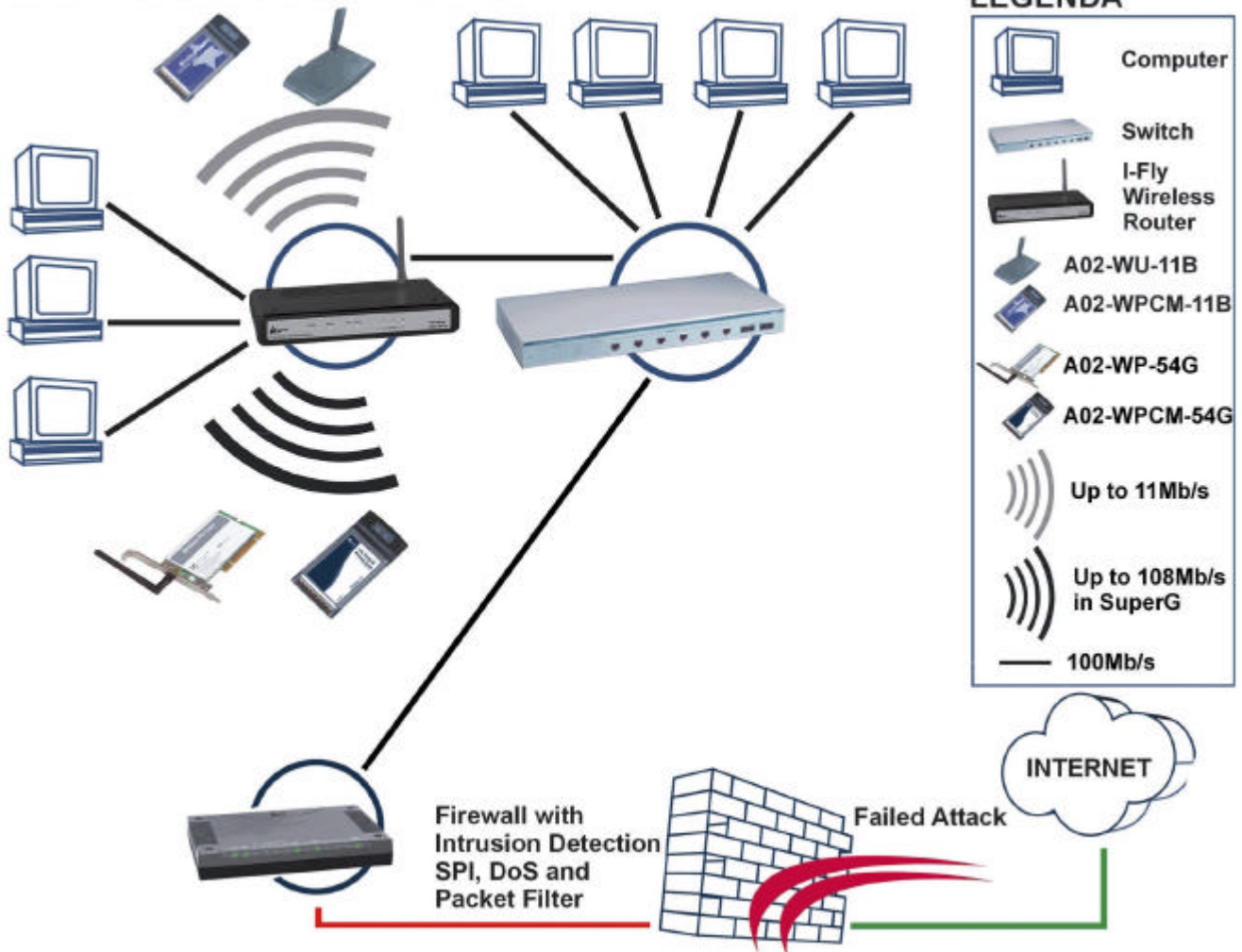
- ? Microsoft Internet Explorer 5.5 or higher
- ? DSL/ Cable Modem Broadband Internet connection and ISP account
- ? PCs equipped with 10Mbps or 10/100 Mbps Ethernet connection to support TCP/IP protocol
- ? One CD-ROM drive

1.5 I-Fly Wireless Broadband Router Application

- ? Home SOHO networking for device sharing and wireless multimedia
- ? Wireless office provides a wider range for home and SOHO Ethernet

- ? Enables wireless building-to-building data communication
- ? Built-in infrastructure mode
- ? Router provides ideal solution for:
 - ? Difficult-to-wire environments
 - ? Temporary LANs for scenarios such as trade-exhibitions and meetings
 - ? Enables LAN adaptability to frequently changing environments
 - ? Enables remote access to corporate network information, for example e-mail and the company home page

WIRELESS ROUTER APPLICATION



LEGENDA

	Computer
	Switch
	I-Fly Wireless Router
	A02-WU-11B
	A02-WPCM-11B
	A02-WP-54G
	A02-WPCM-54G
	Up to 11Mb/s
	Up to 108Mb/s in SuperG
	100Mb/s

2.1 Cautions for using the I-Fly Wireless Broadband Router



Do not place the Router under high humidity and high temperature.

Do not use the same power source for Router with other equipment.

Do not open or repair the case yourself. If the Router is too hot, turn off the power immediately and have a qualified serviceman repair it.



Place the Router on a stable surface.

Only use the power adapter that comes with the package, Using a power supply with a different voltage rating than the one included will cause damage and void the warranty for this product.

2.2 The Front LEDs

LED		MEANING
1	POWER	ON=Indicates proper connection to power supply. OFF= The unit is not receiving power
2	STATUS	BLINKING=Indicates that the device is ready.
3	WAN	ON= Indicates connection to the WAN port BLINKING= Data transmission.
4	WLAN	ON= Link is established BLINKING= Packet transmit or receive activity OFF= No Link activity
5-8	LAN(1,2,3,4)	ON= Indicates connection is established. BLINKING= Data transmissions OFF= No LAN connections

2.3 The Rear Ports



PORT		MEANING
1	LAN (4 connettori RJ-45)	Auto MDI/MDIX LAN ports automatically sense the cable type when connecting to Ethernet-enabled computers.
5	WAN	The Auto MDI/MDIX WAN port is the connection for the Ethernet cable to the Cable or DSL modem
6	RESET	After the device has turned on, press it (10s) to reset the device or restore to factory default settings.
7	POWER (Jack)	Receptor for the Power Adapter

2.4 Cabling

The most common problem is bad cabling or ADSL/ISDN configuration. Make sure that all connected devices are turned on. On the front of the product is a bank of LEDs. As a first check, verify that the LAN/WLAN Link and Power line LEDs are lit. Verify that STATUS blink. If they are not, verify that you are using the proper cables.

Chapter 3

Configuration

The I-Fly Wireless Broadband Router can be configured with your Web browser. The web browser is included as a standard application in the following operation systems, UNIX, Linux, Mac OS, Windows 95/98/NT/2000/Me, and etc. The product provides a very easy and user-friendly interface for configuration.

3.1 Before Configuration

This section describes the configuration required by LAN-attached PCs that communicate with the I-Fly Wireless Broadband Router, either to configure the device or for network access. These PCs must have an Ethernet interface installed properly, be connected to the Router either directly or through an external repeater hub, and have TCP/IP installed and configured to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet of the Router. The default IP address of the ADSL Firewall Router is **192.168.1.1** and subnet mask is 255.255.255.0. The best and easy way is to configure the PC to get an IP address from the Router. Also make sure you have UNINSTALLED any kind of software firewall that can cause problems while accessing the 192.168.1.1 IP address of the router.

Please follow the steps below for PC's network environment installation. First of all, please check your PC's network components. The TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to MS Windows related manuals.



Any TCP/IP capable workstation can be used to communicate with or through the ADSL Firewall Router. To configure other types of workstations, please consult the manufacturer's documentation.

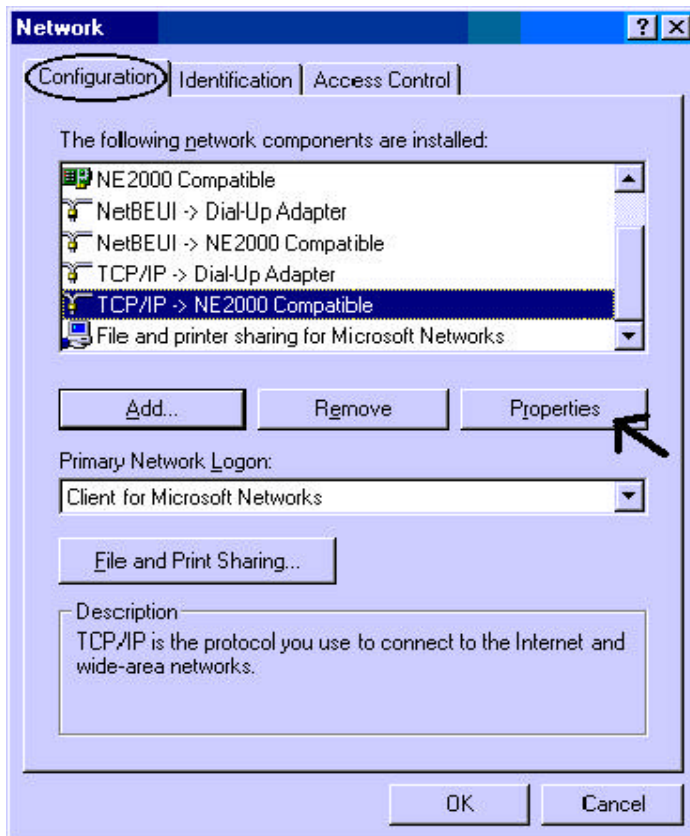
3.2 Connecting the I-Fly Wireless Broadband Router

1. Power on the device
2. Make sure the PWR(green) and SYS(blinking) Leds are OK & LAN(WLAN) Led is lit
3. Connect PC directly to the Router by cable or Wireless
4. Before taking the next step, make sure you have uninstalled any software firewall

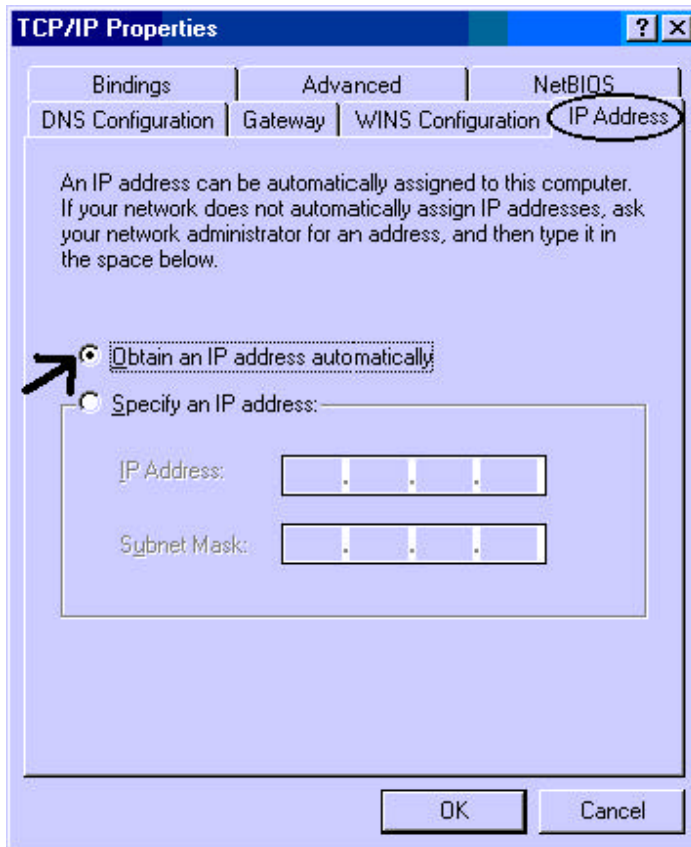
3.3 Configuring PC in Windows

3.3.1 For Windows 95/98/ME

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Configuration** tab.
2. Select **TCP / IP -> NE2000 Compatible**, or the name of any Network Interface Card (NIC) [or Wireless Interface Card in] your PC.
3. Click **Properties**.

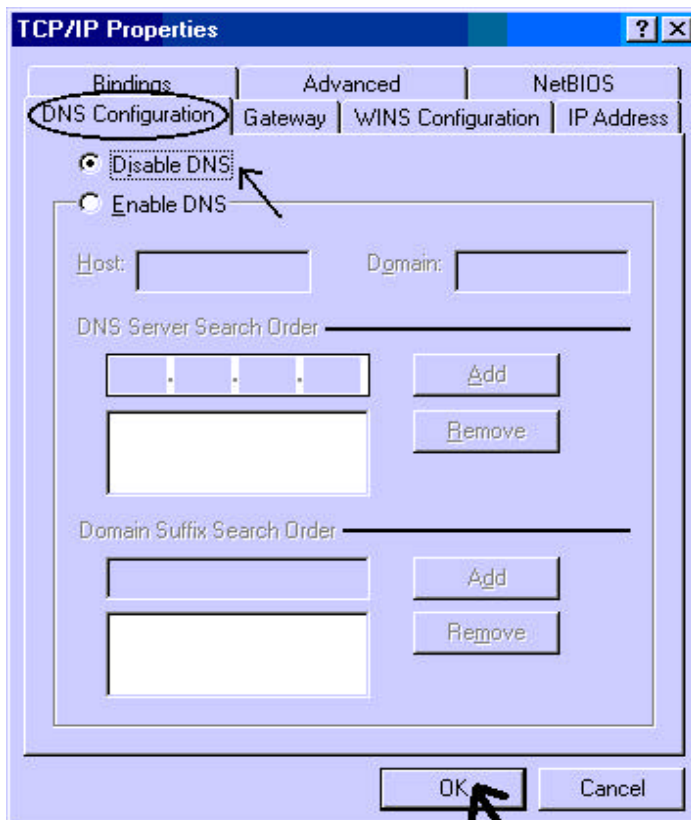


4. Select the **IP Address** tab. In this page, click the **Obtain an IP address automatically** radio button.



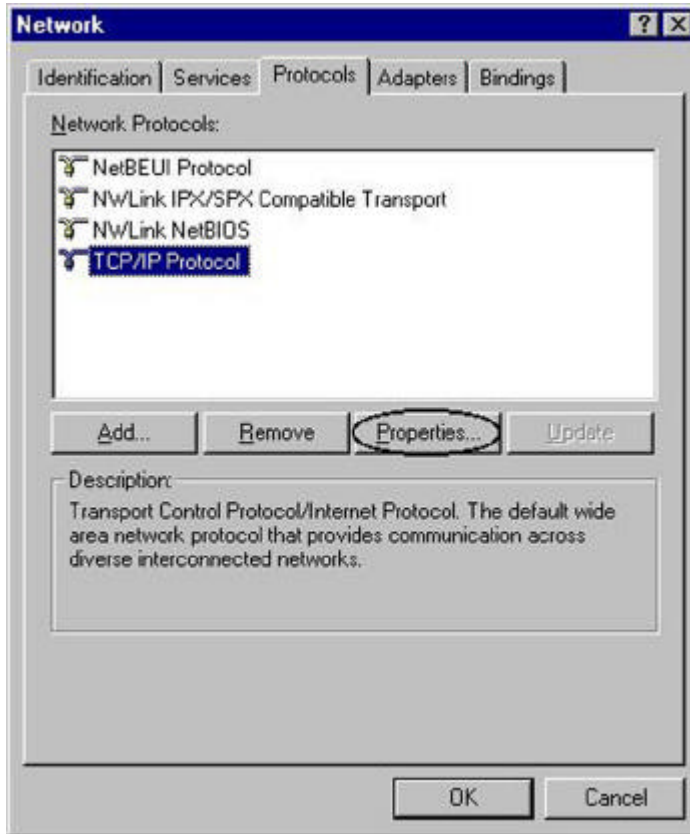
5. Then select the **DNS Configuration** tab.

6. Select the **Disable DNS** radio button and click “OK” to finish the configuration.

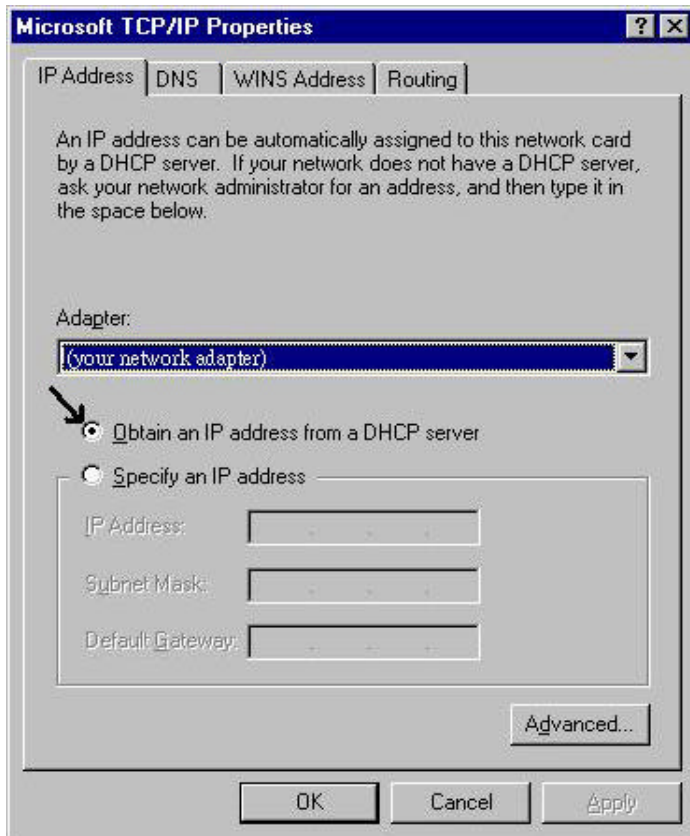


3.3.2 For Windows NT4.0

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Protocols** tab.
2. Select **TCP/IP Protocol** and click **Properties**.



3. Select the **Obtain an IP address from a DHCP server** radio button and click **“OK”**.

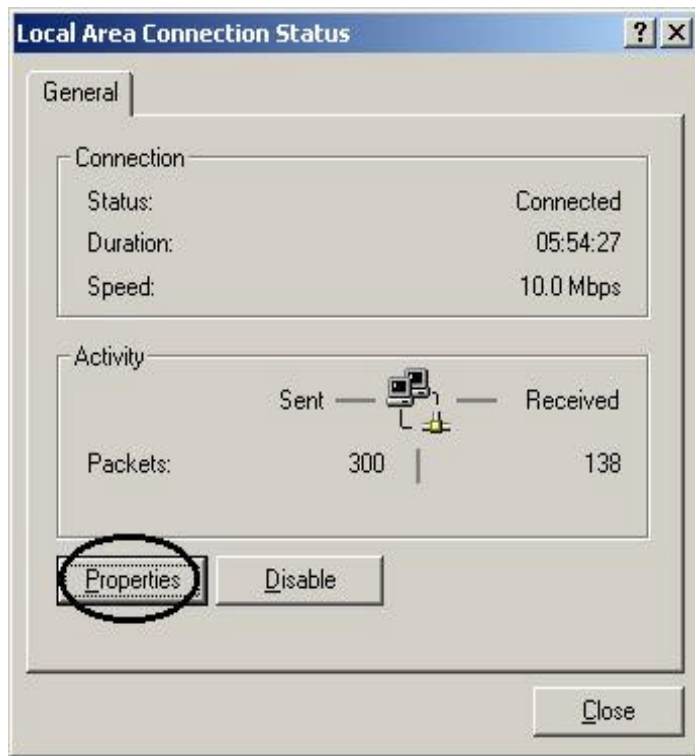


3.3.3 For Windows 2000

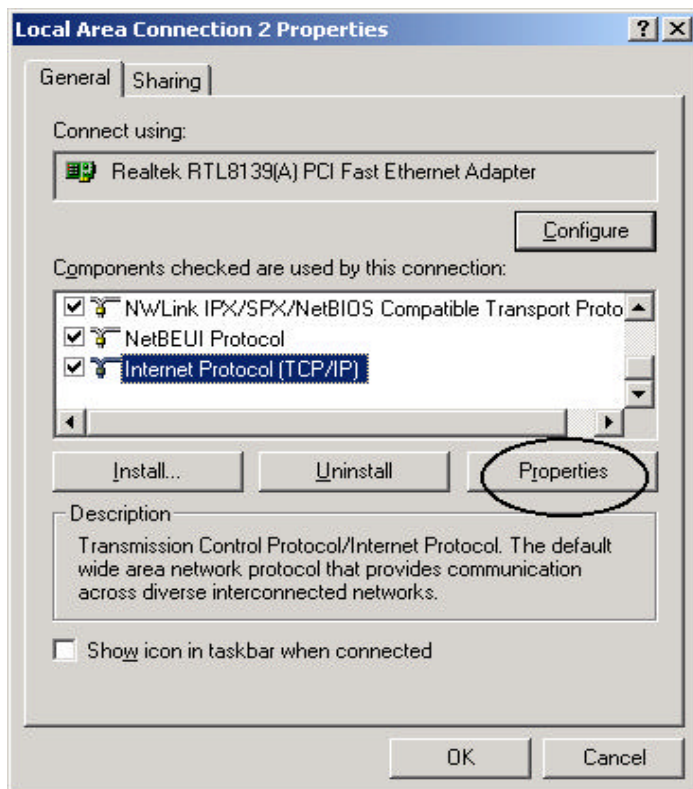
1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network and Dial-up Connections**.
2. Double-click **LAN Area Connection**.



3. In the **LAN Area Connection Status** window, click **Properties**.

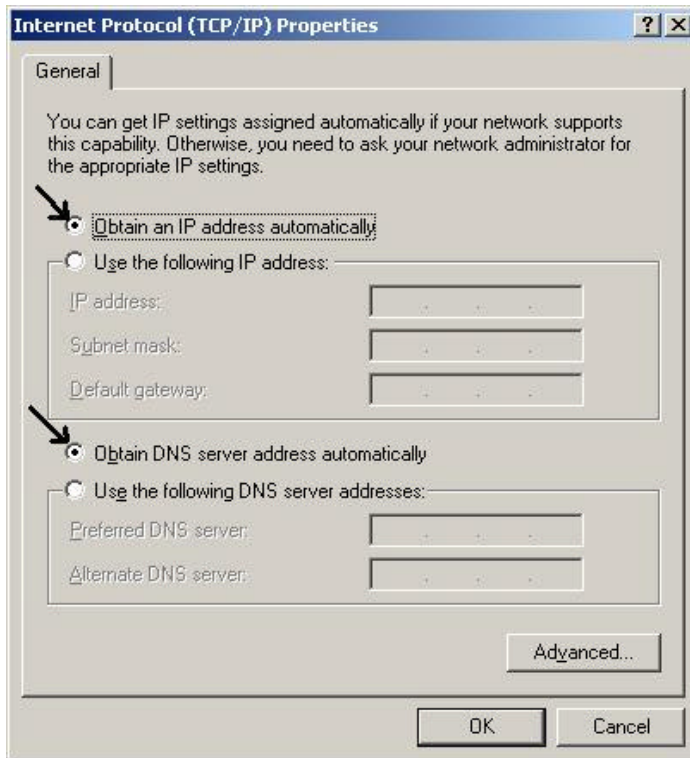


4. Select **Internet Protocol (TCP/IP)** and click **Properties**.



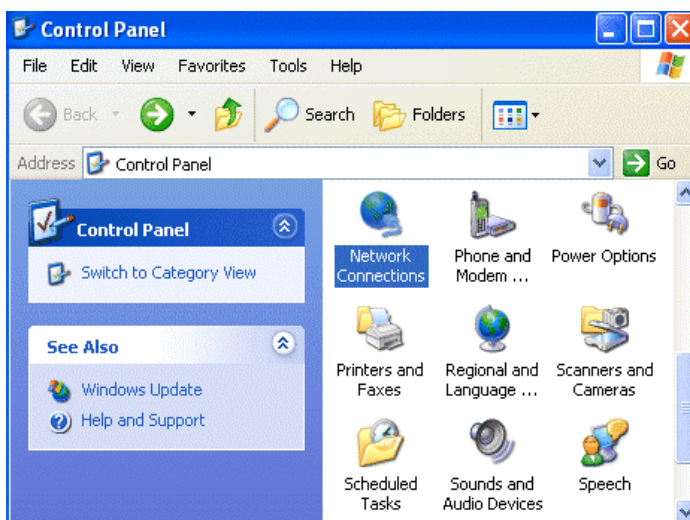
5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.

6. Click **“OK”** to finish the configuration.

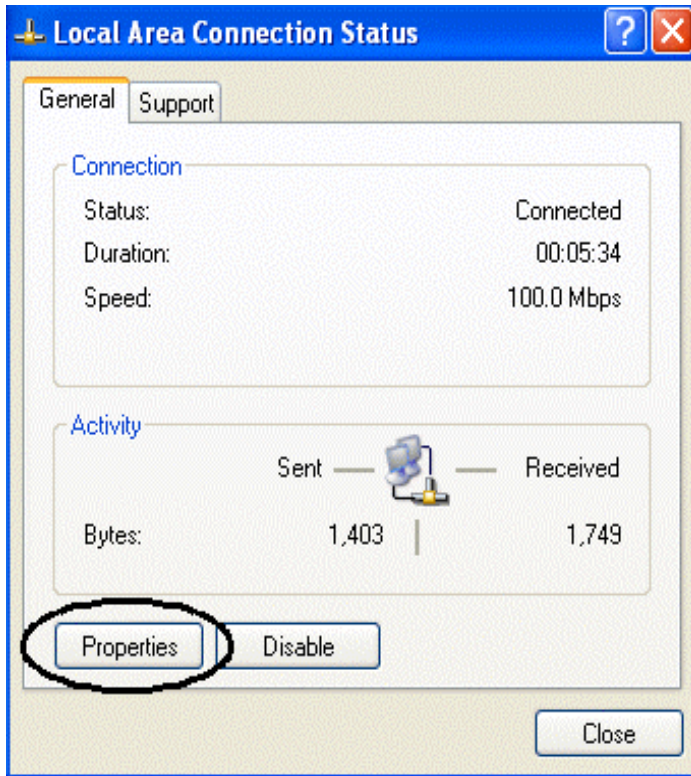


3.3.4 For Windows XP

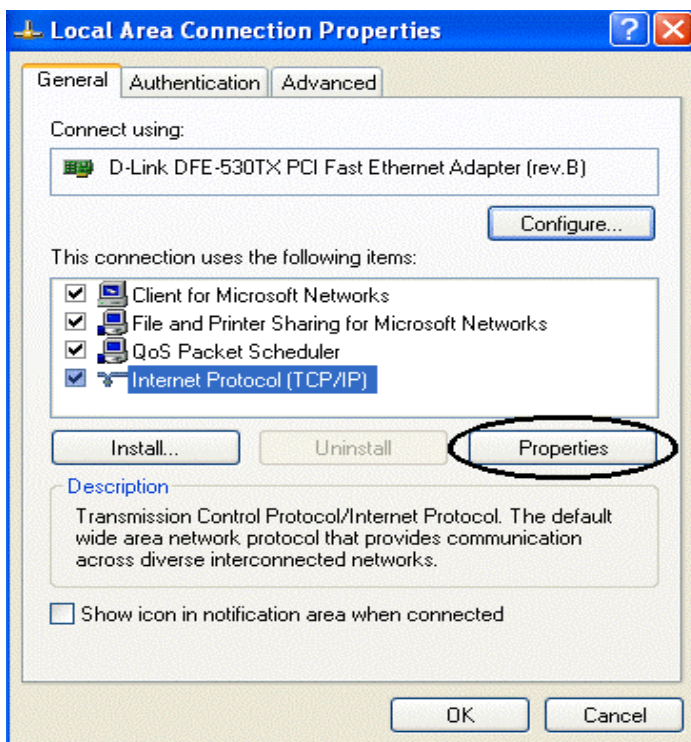
1. Go to **Start / Control Panel** (in Classic View). In the Control Panel, double-click on **Network Connections**.
2. Double-click **Local Area Connection**



3. In the **LAN Area Connection Status** window, click **Properties**.

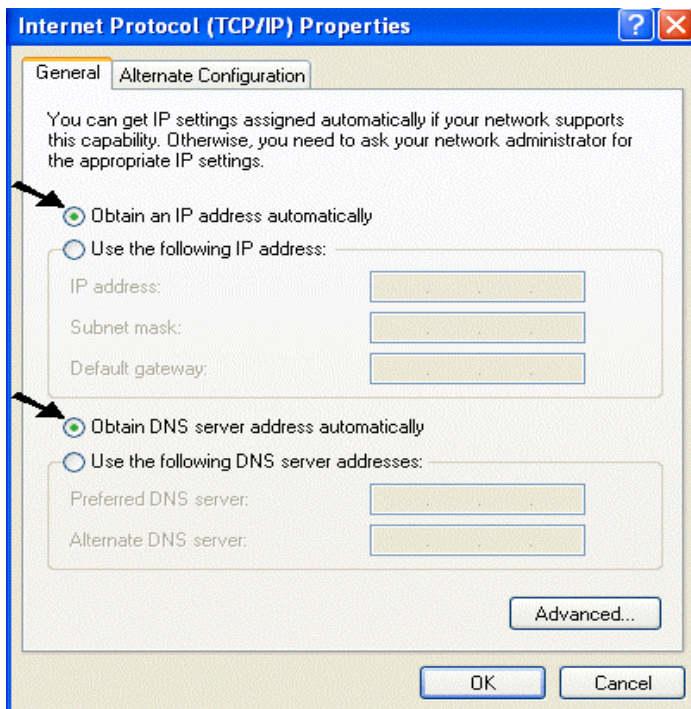


4. Select **Internet Protocol (TCP/IP)** and click **Properties**.



5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons

6. Click **“OK”** to finish the configuration.



3.4 Test TCP/IP

After configuring the TCP/IP protocol, you can use the *ping* command to check if your computer has successfully connected to this Router. The following example shows the ping procedure for Windows 98 .

First, execute the *ping* command.

Ping 192.168.1.1

If the following messages appear:

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 times<10ms TTL=64

Reply from 192.168.1.1: bytes=32 times<10ms TTL=64

Reply from 192.168.1.1: bytes=32 times<10ms TTL=64

A communication link between your computer and this Router has been successfully established.

Otherwise, if you get the following messages,

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

There must be something wrong in configuring procedure or cable issue. Please check the LAN/WLAN LINK LED must be lighted. Or check TCP/IP configuration of your computer.

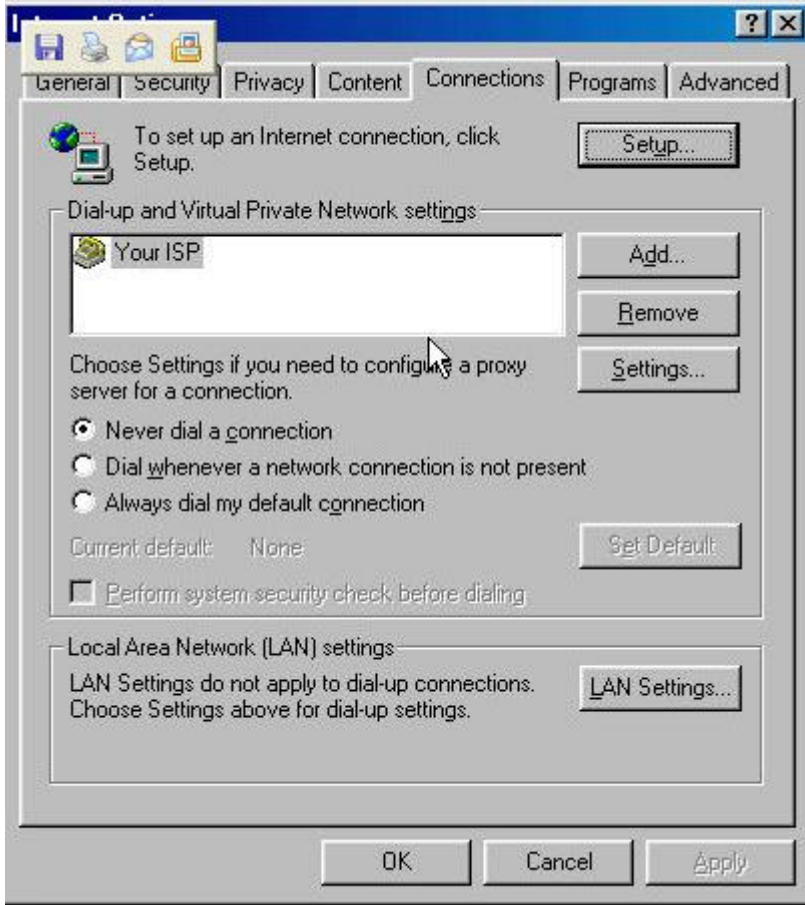
Try to press the key reset for 10 seconds and release it. The router should effect a reboot.

3.5 Configuring Internet Explorer

Click **Tools** on the main menu bar, then click **Internet Options**. The next screen to appear has several tabs across the top.

Select the **Connection** tab.

Chose **Never Dial a Connection** or **Dial whenever a network connection is not present**



3.6 Factory Default Settings

Before configuring this Router, you need to know the following default settings.

Web Configurator

Username : **admin**

Password: **admin**

Device IP Network settings in LAN site

IP Address : **192.168.1.1**

Subnet Mask : **255.255.255.0**

WAN setting : **Client DHCP**

DHCP server : **DHCP server enable**

3.6.1 LAN and WAN Port Addresses

The parameters of LAN and WAN ports are pre-set in the factory. The default values are shown below.

	LAN Port	WAN Port
IP address	192.168.1.1	N/A
Subnet Mask	255.255.255.0	
DHCP server	Enable	

3.7 Reset

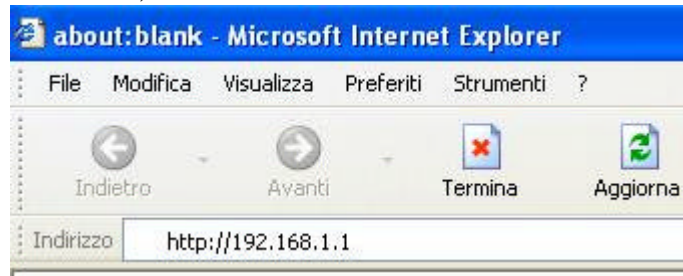
The default username and password are **admin** and **admin** respectively.



If you ever forget the password to log in, you may press the RESET button to restore the factory default settings..

3.8 Configurazione del Router tramite Browser

Open the web browser, enter the local port IP address of this Router, which defaults at **http://192.168.1.1**, and click “Go”,



The below window will popup. Please enter the user name and password. Both of the default is “admin”.



Now, the main menu screen is popup.

The screenshot shows the configuration page for a Wireless Router 54Mbps. The page has a blue header with the router's name and speed. Below the header is a navigation bar with links for LAN&DHCP server, WAN, Password, and Time, along with a HELP button. The main content area is divided into two sections: a left navigation menu and a central configuration form.

The left navigation menu includes the following items:

- LAN Setting
- Wireless
- Status
- Routing
- Access
- Management
- Tools
- Wizard

The central configuration form contains the following fields:

- Host Name: AP-Router
- IP Address: 192.168.1.1
- Subnet Mask: 255.255.255.0
- DHCP Server: Enabled Disabled
- Start IP: 192.168.1.100
- End IP: 192.168.1.199
- Domain Name: (empty)
- Lease Time: 1 Week

Below the form are two buttons: Cancel and Apply. At the bottom of the page is a table listing DHCP profiles:

Host Name	IP Address	MAC Address
unknown	192.168.1.173	00-40-01-20-F4-CD
unknown	192.168.1.128	00-0A-E6-9B-A4-84

At the configuration homepage (if **Quick Setup Wizard** starts, please close it or read the printed Quick Start Guide or read Appendix A), the left navigation page where bookmarks are provided links you directly to the desired setup page, including:

- **LAN Setting**
- **Wireless**
- **Status**
- **Routing**
- **Access**
- **Management**
- **Tools**
- **Wizard**

Click on the desired item to expand the page in the main navigation page.

3.8.1 LAN Settings

The screen enables you to configure the LAN & DHCP Server, set WAN parameters, create Administrator and User passwords, and set the local time, time zone, and dynamic DNS.

3.8.1.1 LAN&DHCP Server

This page enables you to set LAN and DHCP properties, such as the host name, IP address, subnet mask, and domain name. LAN and DHCP profiles are listed in the DHCP table at the bottom of the screen.

LAN&DHCP server ► WAN ► Password ► Time HELP

Host Name	AP-Router
IP Address	192.168.1.251
Subnet Mask	255.255.255.0
DHCP Server	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Start IP	192.168.1.100
End IP	192.168.1.199
Domain Name	
Lease Time	1 Week ▼

Cancel Apply

Host Name	IP Address	MAC Address
unknown	192.168.1.173	00-40-01-20-F4-CD
unknown	192.168.1.128	00-0A-E6-9B-A4-84

Host Name: Type the host name in the text box. The host name is required by some ISPs. The default host name is "AP-Router."

IP Address: This is the IP address of the router. The default IP address is 192.168.1.1.

Subnet Mask: Type the subnet mask for the router in the text box. The default subnet mask is 255.255.255.0.

DHCP Server: Enables the DHCP server to allow the router to automatically assign IP addresses to devices connecting to the LAN. DHCP is enabled by default.

All DHCP client computers are listed in the table at the bottom of the screen, providing the host name, IP address, and MAC address of the client.

Start IP: Type an IP address to serve as the start of the IP range that DHCP will use to assign IP addresses to all LAN devices connected to the router.

End IP: Type an IP address to serve as the end of the IP range that DHCP will use to assign IP addresses to all LAN devices connected to the router.

Domain Name: Type the local domain name of the network in the text box. This item is optional.

Lease Time: Chose the time of lease using the combo box.

3.8.1.2 WAN

This screen enables you to set up the router WAN connection, specify the IP address for the WAN, add DNS numbers, and enter the MAC address.

LAN&DHCP server ► WAN ► Password ► Time HELP

Connection Type	DHCP Client or Fixed IP ▼			
WAN IP	<input checked="" type="radio"/> Obtain IP Automatically			
	<input type="radio"/> Specify IP	IP Address	0.0.0.0	
		Subnet Mask	0.0.0.0	
		Default Gateway	0.0.0.0	
DNS 1	0.0.0.0			
DNS 2	0.0.0.0			
DNS 3	0.0.0.0			
MAC Address	00	- 03	- 2F - 10 - AC - FE	Clone MAC Address

Cancel Apply

Connection Type:

Potrete scegliere tra le seguenti opzioni **DHCP client** or **Fixed IP**, **PPPoE** oppure **PPTP** presenti nel menù a tendina:

Connection Type: Select the connection type, either DHCP client, Fixed IP or PPPoE from the drop-down list.

WAN IP: Select whether you want to specify an IP address manually, or want DHCP to obtain an IP address automatically. When *Specify IP* is selected, type the IP address, subnet mask, and default gateway in the text boxes. Your ISP will provide you with this information.

DNS 1/2/3: Type up to three DNS numbers in the text boxes. Your ISP will provide you with this information.

MAC Address: If required by your ISP, type the MAC address of the router WAN interface in this field.

DNS 1/2/3: Type up to three DNS numbers in the text boxes. Your ISP will provide you with this information.

Connection Type	PPPoE		
WAN IP	<input checked="" type="radio"/> Obtain IP Automatically		
	<input type="radio"/> Specify IP	IP Address	0.0.0.0
DNS 1	0.0.0.0		
DNS 2	0.0.0.0		
DNS 3	0.0.0.0		
User Name			
Password		
Retype Password		
Connect on Demand	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled		
Idle Time Out	0	Minutes	
MTU	1492		

3.8.1.3 Password

This screen enables you to set administrative and user passwords. These passwords are used to gain access to the router interface.

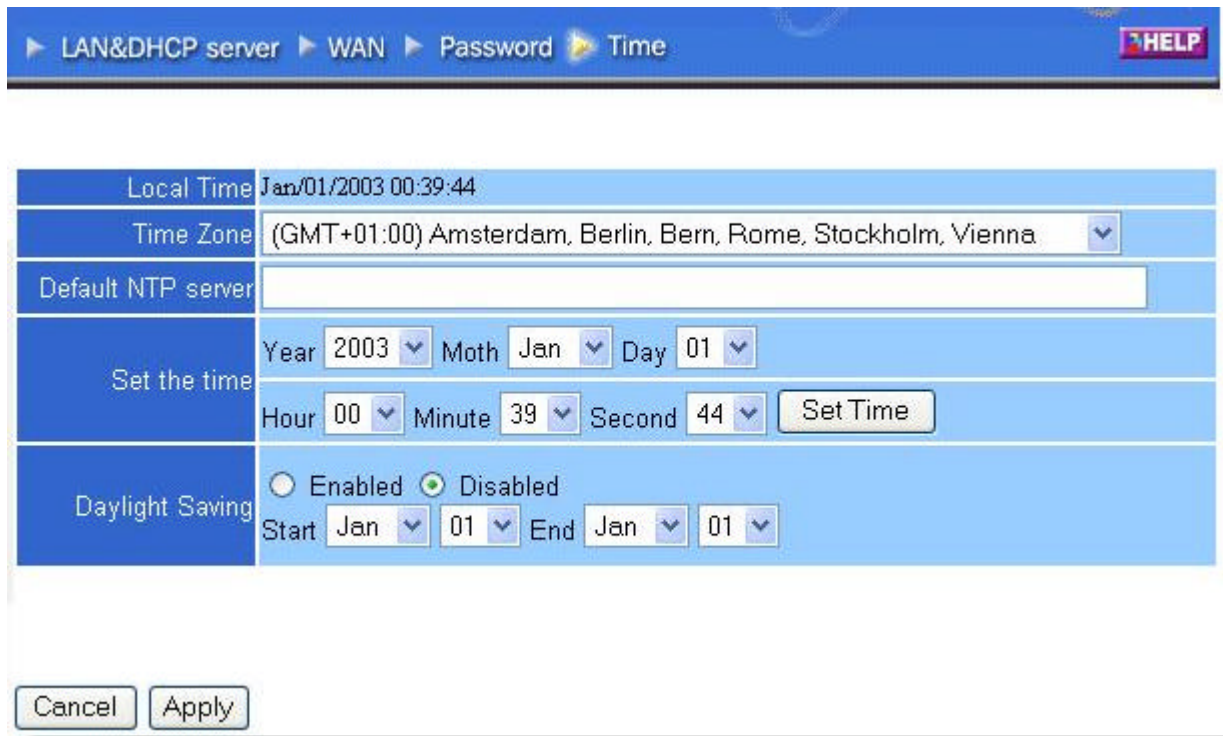
▶ LAN&DHCP server ▶ WAN ▶ Password ▶ Time **HELP**

Administrator (The login name is "admin")	
New Password
Confirm Password
User (The login name is "user")	
New Password
Confirm Password

Administrator: Type the password the Administrator will use to log in to the system. The password must be typed again for confirmation.

3.8.1.4 Time

This screen enables you to set the time and date for the router's real-time clock, select your time zone, and enable or disable daylight saving.



The screenshot shows a web interface for configuring the router's time. At the top, there is a navigation bar with links for LAN&DHCP server, WAN, Password, and Time (which is highlighted), and a HELP button. The main content area is divided into several sections:

- Local Time:** Displays the current local time as Jan/01/2003 00:39:44.
- Time Zone:** A drop-down menu showing "(GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna".
- Default NTP server:** An empty text input field.
- Set the time:** A section with dropdown menus for Year (2003), Month (Jan), and Day (01). Below these are dropdowns for Hour (00), Minute (39), and Second (44), followed by a "Set Time" button.
- Daylight Saving:** Radio buttons for "Enabled" and "Disabled" (which is selected). Below are dropdowns for Start (Jan, 01) and End (Jan, 01).

At the bottom of the form, there are "Cancel" and "Apply" buttons.

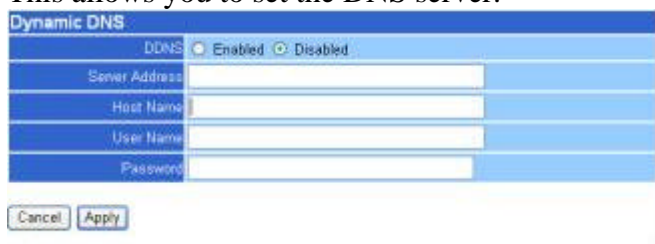
Local Time: Displays the local time and date.

Time Zone: Select your time zone from the drop-down list.

Daylight Saving: Enables you to enable or disable daylight saving time. When enabled, select the start and end date for daylight saving time.

3.8.1.5 Dynamic DNS

This allows you to set the DNS server.



The screenshot shows a web interface for configuring Dynamic DNS. At the top, there is a title "Dynamic DNS" and a section for "DDNS" with radio buttons for "Enabled" (which is selected) and "Disabled". Below this are four text input fields labeled "Server Address", "Host Name", "User Name", and "Password". At the bottom of the form, there are "Cancel" and "Apply" buttons.

3.8.2 Wireless

This section enables you to set wireless communications parameters for the router's wireless LAN feature.

3.8.2.1 Basic

This page allow you to enable and disable the wireless LAN function, create a SSID, and select the channel for wireless communications.

Basic ► WEP ► Advanced ► 802.1X HELP

	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
SSID	Wireless
Channel	9 (Domain: ETSI)

Cancel Apply

Enable/Disable: Enables and disables wireless LAN via the router.

SSID: Type an SSID in the text box. The SSID of any wireless device must match the SSID typed here in order for the wireless device to access the LAN and WAN via the router.

Channel: Select a transmission channel for wireless communications. The channel of any wireless device must match the channel selected here in order for the wireless device to access the LAN and WAN via the router.

3.8.2.2 Authentication

This screen enables you to set authentication type for secure wireless communications. Open System allows public access to the router via wireless communications. Shared Key requires the user to set a WEP key to exchange data with other wireless clients that have the same WEP key.

Basic ► Authentication ► Advanced ► 802.1X HELP

Authentication Type	<input checked="" type="radio"/> Open System <input type="radio"/> Shared Key <input type="radio"/> WPA <input type="radio"/> WPA-PSK
WEP	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Mode	HEX
WEP Key	64-bit
Key 1	<input checked="" type="radio"/> 0000000000
Key 2	<input type="radio"/> 0000000000
Key 3	<input type="radio"/> 0000000000
Key 4	<input type="radio"/> 0000000000

Cancel Apply Clear

Mode: Select the level of encryption you want from the drop-down list. The router supports, 64- and 128-bit encryption.

WEP Key: Select WEP Key - 64 or 128 bits from the drop-down list.

Key 1 ~ Key 4: Enables you to create an encryption scheme for Wireless LAN transmissions.

Manually enter a set of values for each key. Select which key you want to use by clicking the radio button next to the key. Click **Clear** to erase key values.

If WPA is selected, please set the parameters for the RADIUS server. This is also referred to the 802.1X setting.

3.8.2.3 Advanced

This screen enables you to configure advanced wireless functions.

Firmware Version	3.0.0.38	
Beacon Interval	100	(default:100 msec, range:20~1000)
RTS Threshold	2346	(default:2346, range: 1~2346)
Fragmentation Threshold	2346	(default:2346, range: 256~2346, even number only)
DTIM Interval	1	(default:1, range: 1~255)
TX Rates (Mbps)	Auto	
11g only mode	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Antenna transmit power	full	
Super G Mode	Disabled	

Cancel Apply

Beacon Interval: Type the beacon interval in the text box. You can specify a value from 1 to 1000. The default beacon interval is 100.

RTS Threshold: Type the RTS (Request-To-Send) threshold in the text box. This value stabilizes data flow. If data flow is irregular, choose values between 256 and 2432 until data flow is normalized.

Fragmentation Threshold: Type the fragmentation threshold in the text box. If packet transfer error rates are high, choose values between 256 and 2432 until packet transfer rates are minimized. (**NOTE:** set this fragmentation threshold value may diminish system performance.)

DTIM Interval: Type a DTIM (Delivery Traffic Indication Message) interval in the text box. You can specify a value between 1 and 65535. The default value is 3.

TX Rates (Mbps): Select one of the wireless communications transfer rates, measured in megabytes per second, based upon the speed of wireless adapters connected to the WLAN.

11g only mode: enable or disable.

Antenna Power Transmit: Select the Antenna Power transmit for wireless interface.

SuperG: Enable SuperG for superior performance

3.2.3.4 802.1x

There are three essential components to the 802.1x infrastructure: (1) Supplicant, (2) Authenticator and (3) Server. The Router serves as an Authenticator, and the EAP methods used must be supported by the backend Radius Server. The 802.1x security supports both MD5 and TLS Extensive Authentication Protocol (EAP). Please follow the steps below to configure 802.1X security.

1. Enable 802.1X security by selecting “**Enable**”.
2. Select the **Encryption Key Length Size** ranging from 64 to 128 Bits that you would like to use. Select the **Lifetime of the Encryption Key** from 5 Minutes to 1 Day. As soon as the lifetime of the Encryption Key is over, the Encryption Key will be renewed by the Radius server.
3. Enter the **IP address** of and the **Port** used by the **Primary** Radius Server. Enter the **Shared Secret**, which is used by the Radius Server.
4. Enter the **IP address** of, **Port** and **Shared Secret** used by the **Secondary** Radius Server. (Click “**Help**” to get interpretation for Encryption Key and Radius Server.)
5. Click “**Apply**” button for the 802.1x settings to take effect after Wireless router reboots itself.

Note: As soon as 802.1X security is enabled, all the wireless client stations that are connected to the Router currently will be disconnected. The wireless clients must be configured manually to authenticate themselves with the Radius server to be reconnected.

3.8.3 STATUS

This selection enables you to view the status of the router LAN, WAN connections, and view logs and statistics pertaining to connections and packet transfers.

3.8.3.1 Device Information

This screen enables you to view the router LAN, Wireless and WAN configuration.

Firmware Version: Displays the latest build of the router firmware interface. After updating the firmware in Tools - Firmware, check this to ensure that your firmware was successfully updated.

LAN: This field displays the router's LAN interface MAC address, IP address, subnet mask, and DHCP server status. Click *DHCP Table* to view a list of client stations currently connected to the router LAN interface.

Wireless: Displays the router's wireless connection information, including the router's wireless interface MAC address, the connection status, the SSID status, which channel is being used, and whether WEP is enabled or not.

WAN: This field displays the router's WAN interface MAC address, DHCP client status, IP address, subnet mask, default gateway, and DNS.

Click *DHCP Release* to release all IP addresses assigned to client stations connected to the WAN via the router. Click *DHCP Renew* to reassign IP addresses to client stations connected to the WAN.

[Device information](#) ▶ [Log](#) ▶ [Log Setting](#) ▶ [Statistic](#) ▶ [Wireless](#) **HELP**

Firmware Version: 1.1.7 , 2003/06/09

LAN	
MAC Address	00-03-2F-10-AC-FD
IP Address	192.168.1.251
Subnet Mask	255.255.255.0
DHCP Server	Enabled DHCP Table

Wireless	
MAC Address	00-40-05-56-1A-05
Connection	802.11g AP Enable
ESSID	Wireless
Channel	9
WEP	DISABLE

WAN	
MAC Address	00-03-2F-10-AC-FE
Connection	DHCP client Disconnected <input type="button" value="DHCP Release"/> <input type="button" value="DHCP Renew"/>
IP	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
DNS	

3.8.3.2 Log

This screen enables you to view a running log of router system statistics, events, and activities. The log displays up to 200 entries. Older entries are overwritten by new entries. The Log screen commands are as follows:

Click *First Page* to view the first page of the log

Click *Last Page* to view the final page of the log

Click *Previous Page* to view the page just before the current page

Click *Next Page* to view the page just after the current page

Click *Clear Log* to delete the contents of the log and begin a new log

Click *Refresh* to renew log statistics



Time: Displays the time and date that the log entry was created.

Message: Displays summary information about the log entry.

Source: Displays the source of the communication.

Destination: Displays the destination of the communication.

Note: Displays the IP address of the communication

3.8.3.3 Log Setting

This screen enables you to set router logging parameters.



SMTP Server: Type the SMTP server address for the email that the log will be sent to in the next field.

Send to: Type an email address for the log to be sent to. Click *Email Log Now* to immediately send the current log.

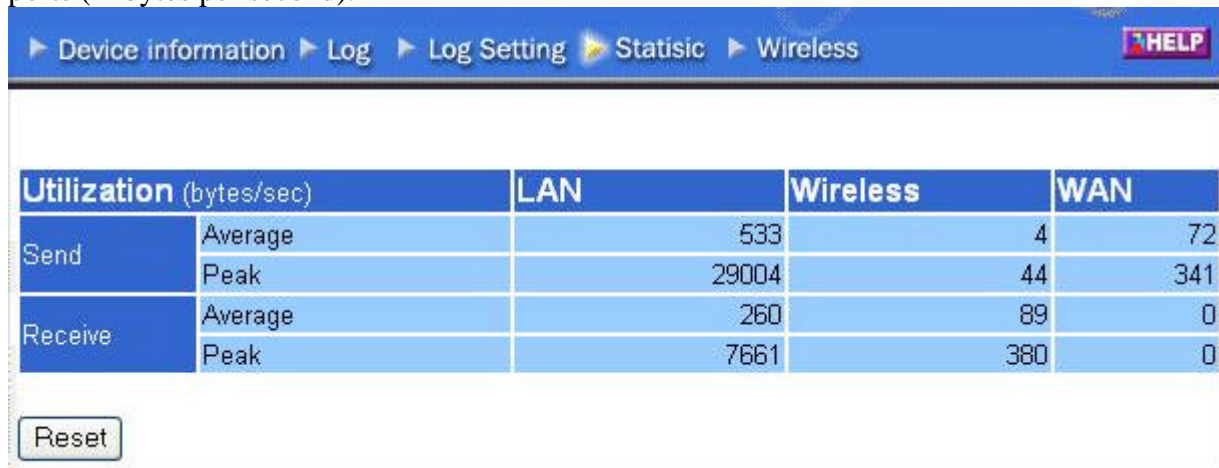
Syslog Server: Type the IP address of the Syslog Server if you want the router to listen and receive incoming Syslog messages.

Log Type: Enables you to select what items will be included in the log:

- ? System Activity: Displays information related to router operation.
- ? Debug Information: Displays information related to errors and system malfunction.
- ? Attacks: Displays information about any malicious activity on the network.
- ? Dropped Packets: Displays information about packets that have not been transferred successfully.
- ? Notice: Displays important notices by the system administrator.

3.8.3.4 Statistics

This screen displays a table that shows the rate of packet transmission via the router LAN and WAN ports (in bytes per second).



Utilization (bytes/sec)		LAN	Wireless	WAN
Send	Average	533	4	72
	Peak	29004	44	341
Receive	Average	260	89	0
	Peak	7661	380	0

Reset

Click *Reset* to erase all statistics and begin logging statistics again.

3.8.3.5 Wireless

This screen enables you to view information about wireless devices that are connected to the wireless router.

Connected Time: Displays how long the wireless device has been connected to the LAN via the router.

MAC Address: Displays the devices wireless LAN interface MAC address.

3.8.4 ROUTING

This selection enables you to set how the router forwards data: Static and Dynamic. Routing Table enables you to view the information created by the router that displays the network interconnection topology.

3.8.4.1 Static

It enables you to set parameters by which the router forwards data to its destination if your network has a static IP address.

Static Dynamic Routing Table HELP

Network Address	<input type="text"/>
Network Mask	<input type="text"/>
Gateway Address	<input type="text"/>
Interface	LAN <input type="button" value="v"/>
Metric	<input type="text"/>

Network Address	Mask	Gateway	Interface	Metric
-----------------	------	---------	-----------	--------

Network Address: Type the static IP address your network uses to access the Internet. Your ISP or network administrator provides you with this information.

Network Mask: Type the network (subnet) mask for your network. If you do not type a value here, the network mask defaults to 255.255.255.255. Your ISP or network administrator provides you with this information.

Gateway Address: Type the gateway address for your network. Your ISP or network administrator provides you with this information.

Interface: Select which interface, WAN or LAN, you use to connect to the Internet.

Metric: Select which metric you want to apply to this configuration.

Add: Click to add the configuration to the static IP address table at the bottom of the page.

Update: Select one of the entries in the static IP address table at the bottom of the page and, after changing parameters, click *Update* to confirm the changes.

Delete: Select one of the entries in the static IP address table at the bottom of the page and click *Delete* to remove the entry.

New: Click *New* to clear the text boxes and add required information to create a new entry.

3.8.4.2 Dynamic

This screen enables you to set NAT parameters and RIP V1 and RIP V2.

Static Dynamic Routing Table HELP

NAT	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Transmit	<input type="radio"/> Disabled <input type="radio"/> RIP 1 <input type="radio"/> RIP 2
Receive	<input checked="" type="radio"/> Disabled <input type="radio"/> RIP 1 <input type="radio"/> RIP 2

NAT: Click the radio buttons to enable or disable NAT.

Transmit: Click the radio buttons to set the desired transmit parameters, disabled, RIP 1, or RIP 2.

Receive: Click the radio buttons to set the desired transmit parameters, disabled, RIP 1, or RIP 2

3.8.4.3 Routing Table

This screen enables you to view the routing table for the router. The routing table is a database created by the router that displays the network interconnection topology.

Network Address: Displays the network IP address of the connected node.

Network Mask: Displays the network (subnet) mask of the connected node.

Gateway Address: Displays the gateway address of the connected node.

Interface: Displays whether the node is connected via a WAN or LAN.

Metric: Displays the metric of the connected node.

Type: Displays whether the node has a static or dynamic IP address

3.8.5 Access

This page enables you to define access restrictions, set up protocol and IP filters, create virtual servers, define access for special applications such as games, and set firewall rules.

3.8.5.1 Filter

Using filters to deny or allow the users to access. Five types of filters to select: MAC, URL blocking, IP, Protocol filter and Domain blocking.

Filters > Virtual Server > Special AP > DMZ > Firewall Rule HELP

Filters

Filters are used to allow or deny LAN users from accessing the internet.

MAC Filters URL Blocking
 IP Filters Domain Blocking Protocol Filters

MAC Filter

Disabled
 Enable

Apply

MAC Table

Name:

MAC Address: - - - - -

Add Update Delete Clear

Name	MAC Address	Connection
------	-------------	------------

MAC Filter

MAC Filter

Disabled
 Enable

Apply

MAC Table

Name	<input type="text"/>
MAC Address	<input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/>

Add Update Delete Clear

MAC Filter: Enables you to allow or deny Internet access to users within the LAN based upon the MAC address of their network interface. Click the radio button next to *Disabled* to disable the MAC filter.

Disable: Once the function of MAC filter is disabled, those listed in the MAC Table are allowed Internet access.

Enable: All users are allowed Internet access except those user in the MAC Table are deny Internet access.

MAC Table: Use this section to create a user profile which Internet access is denied or allowed. The user profiles are listed in the table at the bottom of the page. (**Note:** Click anywhere in the item. Once the line is selected, the fields automatically load the item's parameters, which you can edit.)

Name: Type the name of the user to be permitted/denied access.

MAC Address: Type the MAC address of the user's network interface.

Add: Click to add the user to the list at the bottom of the page.

Update: Click to update information for the user, if you have changed any of the fields.

Delete: Select a user from the table at the bottom of the list and click *Delete* to remove the user profile.

New: Click *New* to erase all fields and enter new information.

URL Blocking

You could enable URL blocking to deny the users from accessing the specified URL. Add those specified URL in the text box.

Filters

Filters are used to allow or deny LAN users from accessing the Internet.

MAC Filters URL Blocking
 IP Filters Domain Blocking Protocol Filters

URL Blocking

Block those URLs which contain keywords listed below.

Enabled Disabled

Add Update Delete Clear

IP Filter

This screen enables you to define a minimum and maximum IP address range filter; all IP addresses falling in the range are not allowed Internet access. The IP filter profiles are listed in the table at the

bottom of the page. (**Note:** Click anywhere in the item. Once the line is selected, the fields automatically load the item's parameters, which you can edit.)

Enable	<input type="radio"/> Enable <input type="radio"/> Disabled
Range Start	<input type="text"/>
Range End	<input type="text"/>

Enable: Click to enable or disable the IP address filter.

Range Start: Type the minimum address for the IP range. IP addresses falling between this value and the Range End are not allowed to access the Internet.

Range End: Type the minimum address for the IP range. IP addresses falling between this value and the Range Start are not allowed to access the Internet.

Add: Click to add the IP range to the table at the bottom of the screen.

Update: Click to update information for the range if you have selected a list item and have made changes.

Delete: Select a list item and click *Delete* to remove the item from the list.

New: Click *New* to erase all fields and enter new information.

Protocol Filter

This screen enables you to allow and deny access based upon a communications protocol list you create. The protocol filter profiles are listed in the table at the bottom of the page.

Note: When selecting items in the table at the bottom, click anywhere in the item. The line is selected, and the fields automatically load the item's parameters, which you can edit:

Filters
Filters are used to allow or deny LAN users from accessing the Internet.

MAC Filters URL Blocking
 IP Filters Domain Blocking Protocol Filters

Protocol Filter
 Disable List
 Enable List: Deny to access internet from LAN when

Edit protocol Filter in List

Enable Enable Disabled

Name

Protocol TCP

Port - (Type Range for ICMP)

Protocol Filter

Disable List

Enable List : Deny to access internet from LAN when the list as below item be enable.

Apply

Edit protocol Filter in List

Enable Enable Disabled

Name

Protocol ▼

Port Range - (Type Range for ICMP)

Add Update Delete New

	Name	Protocol	Range
<input checked="" type="checkbox"/>	Filter FTP	TCP	20-21
<input type="checkbox"/>	Filter HTTP	TCP	80
<input type="checkbox"/>	Filter HTTPS	TCP	443
<input type="checkbox"/>	Filter DNS	UDP	53
<input type="checkbox"/>	Filter SMTP	TCP	25
<input type="checkbox"/>	Filter POP3	TCP	110
<input type="checkbox"/>	Filter Ping	ICMP	8
<input type="checkbox"/>	Filter Telnet	TCP	23

Domain Blocking

You could specify the domains which allow users to access or deny by clicking one of the two items. Also, add the specified domains in the text box.

Filters

Filters are used to allow or deny LAN users from accessing the Internet.

MAC Filters URL Blocking

IP Filters Domain Blocking Protocol Filters

Domain Blocking

Disabled

Allow users to access all domains except "Blocked Domains"

Deny users to access all domains except "Permitted Domains"

Permitted Domains

Delete

Blocked Domains

Delete

3.8.5.2 Virtual Server

This screen enables you to create a virtual server via the router. If the router is set as a virtual server, remote users requesting Web or FTP services through the WAN are directed to local servers in the LAN. The router redirects the request via the protocol and port numbers to the correct LAN server. The Virtual Sever profiles are listed in the table at the bottom of the page.

Note: When selecting items in the table at the bottom, click anywhere in the item. The line is selected, and the fields automatically load the item's parameters, which you can edit.

Enable	<input type="radio"/> Enable <input type="radio"/> Disabled		
Name	<input type="text"/>		
Protocol	TCP ▾		
Private Port	<input type="text"/>		
Public Port	<input type="text"/>		
LAN Server	<input type="text"/>		

	Name	Protocol	LAN Server
<input type="checkbox"/>	Virtual Server FTP	TCP 21/21	0.0.0.0
<input type="checkbox"/>	Virtual Server HTTP	TCP 80/80	0.0.0.0
<input type="checkbox"/>	Virtual Server HTTPS	TCP 443/443	0.0.0.0
<input type="checkbox"/>	Virtual Server DNS	UDP 53/53	0.0.0.0
<input type="checkbox"/>	Virtual Server SMTP	TCP 25/25	0.0.0.0
<input type="checkbox"/>	Virtual Server POP3	TCP 110/110	0.0.0.0
<input type="checkbox"/>	Virtual Server Telnet	TCP 23/23	0.0.0.0
<input type="checkbox"/>	IPSec	UDP 500/500	0.0.0.0
<input type="checkbox"/>	PPTP	TCP 1723/1723	0.0.0.0

Enable: Click to enable or disable the virtual server.

Name: Type a descriptive name for the virtual server.

Protocol: Select the protocol (TCP or UDP) you want to use for the virtual server.

Private Port: Type the port number of the computer on the LAN that is being used to act as a virtual server.

Public Port: Type the port number on the WAN that will be used to provide access to the virtual server.

LAN Server: Type the LAN IP address that will be assigned to the virtual server.

Add: Click to add the virtual server to the table at the bottom of the screen.

Update: Click to update information for the virtual server if you have selected a list item and have made changes.

Delete: Select a list item and click *Delete* to remove the item from the list.

New: Click *New* to erase all fields and enter new information.

	Name	Protocol	LAN Server
<input type="checkbox"/>	Virtual Server FTP	TCP 21/21	0.0.0.0
<input checked="" type="checkbox"/>	Virtual Server HTTP	TCP 80/80	192.168.1.2
<input type="checkbox"/>	Virtual Server HTTPS	TCP 443/443	0.0.0.0
<input type="checkbox"/>	Virtual Server DNS	UDP 53/53	0.0.0.0
<input type="checkbox"/>	Virtual Server SMTP	TCP 25/25	0.0.0.0
<input type="checkbox"/>	Virtual Server POP3	TCP 110/110	0.0.0.0
<input type="checkbox"/>	Virtual Server Telnet	TCP 23/23	0.0.0.0
<input type="checkbox"/>	IPSec	UDP 500/500	0.0.0.0
<input type="checkbox"/>	PPTP	TCP 1723/1723	0.0.0.0

Application	Outgoing	Ingoing
ICQ 98, 99a	Nessuno	Nessuno
NetMeeting 2.1 a 3.01	Nessuno	1503 TCP, 1720 TCP
VDO Live	Nessuno	Nessuno
mIRC	Nessuno	Nessuno
Cu-SeeMe	7648 TCP &UDP, 24032 UDP	7648 TCP &UDP, 24032 UDP
PC AnyWhere	5632 UDP, 22 UDP, 5631 TCP, 65301 TCP	5632 UDP, 22 UDP, 5631 TCP, 65301 TCP
Edonkey/Emule	Nessuno	principalmente 4660-4662 TCP , 4665 UDP
MSN Messenger	Nessuno	TCP da 6891-6900 TCP 1863 TCP 6901 UDP 1863 UDP 6901 UDP 5190

Service	N° Port / Protocol
File Transfer Protocol (FTP) Data	20/tcp
FTP Commands	21/tcp
Telnet	23/tcp
Simple Mail Transfer Protocol (SMTP) Email	25/tcp
Domain Name Server (DNS)	53/tcp and 53/udp
Trivial File Transfer Protocol (TFTP)	69/udp
finger	79/tcp
World Wide Web (HTTP)	80/tcp
POP3 Email	110/tcp
SUN Remote Procedure Call (RPC)	111/udp
Network News Transfer Protocol (NNTP)	119/tcp
Network Time Protocol (NTP)	123/tcp and 123/udp
News	144/tcp
Simple Management Network Protocol (SNMP)	161/udp
SNMP (traps)	162/udp
Border Gateway Protocol (BGP)	179/tcp
Secure HTTP (HTTPS)	443/tcp
rlogin	513/tcp
rexec	514/tcp
talk	517/tcp and 517/udp
ntalk	518/tcp and 518/udp
Open Windows	2000/tcp and 2000/udp
Network File System (NFS)	2049/tcp
X11	6000/tcp and 6000/udp
Routing Information Protocol (RIP)	520/udp
Layer 2 Tunnelling Protocol (L2TP)	1701/udp

3.8.5.3 Special AP

This screen enables you to specify special applications, such as games, that require multiple connections that are inhibited by NAT. The special applications profiles are listed in the table at the bottom of the page.

Note: When selecting items in the table at the bottom, click anywhere in the item. The line is selected, and the fields automatically load the item's parameters, which you can edit.

Enable	<input type="radio"/> Enabled <input type="radio"/> Disabled	
Name	<input type="text"/>	
Trigger	Protocol	TCP <input type="button" value="v"/>
	Port Range	<input type="text"/> - <input type="text"/>
Incoming	Protocol	TCP <input type="button" value="v"/>
	Port	<input type="text"/>

	Name	Triger Port Range	Incoming Port
<input type="checkbox"/>	Battle.net	6112	6112
<input type="checkbox"/>	Dialpad	7175	51200-51201,51210
<input type="checkbox"/>	ICU II	2019	2000-2038,2050-2051,2069,2085,3010-3030
<input type="checkbox"/>	MSN Gaming Zone	47624	2300-2400,28800-29000
<input type="checkbox"/>	PC-to-Phone	12053	12120,12122,24150-24220
<input type="checkbox"/>	Quick Time 4	554	6970-6999

Enable: Click to enable or disable the application profile. When enabled, users will be able to connect to the application via the router WAN connection. Click Disabled on a profile to prevent users from accessing the application on the WAN.

Name: Type a descriptive name for the application.

Trigger: Defines the outgoing communication that determines whether the user has legitimate access to the application.

? **Protocol:** Select the protocol (TCP, UDP, or ICMP) that can be used to access the application.

? **Port Range:** Type the port range that can be used to access the application in the text boxes.

Incoming: Defines which incoming communications users are permitted to connect with.

? **Protocol:** Select the protocol (TCP, UDP, or ICMP) that can be used by the incoming communication.

? **Port:** Type the port number that can be used for the incoming communication.

Add: Click to add the special application profile to the table at the bottom of the screen.

Update: Click to update information for the special application if you have selected a list item and have made changes.

Delete: Select a list item and click *Delete* to remove the item from the list.

New: Click *New* to erase all fields and enter new information.

3.8.5.4 DMZ

This screen enables you to create a DMZ for those computers that cannot access Internet applications properly through the router and associated security settings.

Note: Any clients added to the DMZ exposes the clients to security risks such as viruses and unauthorized access.

Mac Filter > Protocol Filter > IP Filter > Virtual Server > Special AP > DMZ > Firewall Rule **HELP**

Enable Enabled Disabled

DMZ Host IP

Apply

Enable: Click to enable or disable the DMZ.

DMZ Host IP: Type a host IP address for the DMZ. The computer with this IP address acts as a DMZ host with unlimited Internet access.

Apply: Click to save the settings.

3.8.5.5 Firewall Rule

This screen enables you to set up the firewall. The router provides basic firewall functions, by filtering all the packets that enter the router using a set of rules. The rules are in an order sequence list--the lower the rule number, the higher the priority the rule has.

Enable Enable Disabled

Name

Action Allow Deny

	Interface	IP Range Start	IP Range End	Protocol	Port Range
Source	* <input type="text"/>	<input type="text"/>	<input type="text"/>		
Destination	* <input type="text"/>	<input type="text"/>	<input type="text"/>	TCP <input type="text"/>	<input type="text"/> - <input type="text"/>

Add Update Delete **New** Priority Up Priority Down Update Priority

Enable: Click to enable or disable the firewall rule profile.

Name: Type a descriptive name for the firewall rule profile.

Action: Select whether to allow or deny packets that conform to the rule.

Inactive Timeout: Type the number of seconds of network inactivity that elapses before the router refuses the incoming packet.

Source: Defines the source of the incoming packet that the rule is applied to.

? **Interface:** Select which interface (WAN or LAN) the rule is applied to.

? **IP Range Start:** Type the start IP address that the rule is applied to.

? **IP Range End:** Type the end IP address that the rule is applied to.

Destination: Defines the destination of the incoming packet that the rule is applied to.

? **Interface:** Select which interface (WAN or LAN) the rule is applied to.

? **IP Range Start:** Type the start IP address that the rule is applied to.

? **IP Range End:** Type the end IP address that the rule is applied to.

? **Protocol:** Select the protocol (TCP, UDP, or ICMP) of the destination.

? **Port Range:** Select the port range.

Add: Click to add the rule profile to the table at the bottom of the screen.

Update: Click to update information for the rule if you have selected a list item and have made changes.

Delete: Select a list item and click *Delete* to remove the item from the list.

New: Click *New* to erase all fields and enter new information.

Priority Up: Select a rule from the list and click *Priority Up* to increase the priority of the rule.

Priority Down: Select a rule from the list and click *Priority Down* to decrease the priority of the rule.

Update Priority: After increasing or decreasing the priority of a rule, click *Update Priority* to save the changes.

3.8.6 Management

Management enables you to set up SNMP and Remote Management feature.

3.8.6.1 SNMP

This screen enables you to configure SNMP.

<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	
System Name	AP-Router
System Location	
System Contact	
Community	
Trap Receiver 1	0.0.0.0
2	0.0.0.0
3	0.0.0.0

Cancel Apply

Enabled/Disabled: Click to enable or disable SNMP.

System Name: Displays the name given to the router.

System Location: Displays the location of the router (normally, the DNS name).

System Contact: Displays the contact information for the person responsible for the router.

Community: SNMP system name for exchanging SNMP community messages. The name can be used to limit SNMP messages passing through the network. The default name is 'public.'

Trap Receiver: Type the name of the destination PC that will receive trap messages.

3.8.6.2 Remote Management

This screen enables you to set up remote management. Using remote management, the router can be configured through the WAN via a Web browser. A user name and password are required to perform remote management.

HTTP	Enable	<input type="radio"/> Enable	<input checked="" type="radio"/> Disabled
	port	8080	
	Remote IP Range	From *	To

HTTP: Enables you to set up HTTP access for remote management.

? **Enable:** Click to enable or disable HTTP access for remote management.

- **Port:** Select the port
- **Remote IP Range:** Type the start IP and END addresses.

Allow to Ping WAN Port	Enable	<input type="radio"/> Enable	<input checked="" type="radio"/> Disabled
	Remote IP Range	From *	To

Allow to Ping WAN Port: Type a range of router IP addresses that can be pinged from remote locations

- **Enable/Disable**
- **Remote IP Range:** Type the start IP and END addresses

UPNP Enable	Enable	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
Gaming mode	Enable	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
PPTP	Enable	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
IPSec	Enable	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
IDENT	Enable	<input checked="" type="radio"/> Closed	<input type="radio"/> Stealth

UPNP: UPNP is short for Universal Plug and Play which is a networking architecture that provides compatibility among networking equipment, software, and peripherals. The Router is a UPnP enabled router and will only work with other UPnP devices/software. If you do not want to use the UPnP functionality, it can be disabled by selecting "Disabled".

GAMING MODE: If you are experiencing difficulties when playing online games or even certain applications that use voice data, you may need to enable Gaming Mode for these applications to work correctly. When not playing games or using these voice applications, it is recommended that Gaming Mode is disabled.

PPTP: Enables you to set up PPTP access for remote management.

IPSec: Enables you to set up IPSec access for remote management.

IDENT: Default is closed. This enables you to set port 113 stealth.

3.8.7 Tools

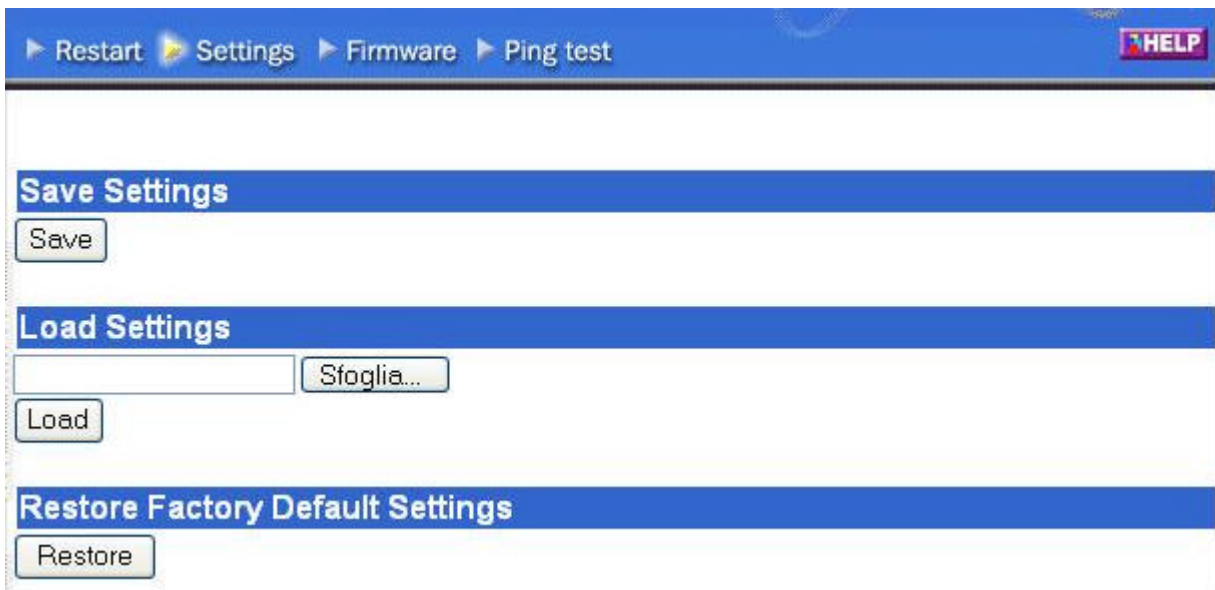
This page enables you to restart the system, save and load different settings as profiles, restore factory default settings, run a setup wizard to configure router settings, upgrade the firmware, and ping remote IP addresses.

3.8.7.1 Restart

Click *Restart* to restart the system in the event the system is not performing correctly.

3.8.7.2 Settings

This screen enables you to save your settings as a profile and load profiles for different circumstances. You can also load the factory default settings, and run a setup wizard to configure the router and router interface.



Save Settings: Click to save the current configuration as a profile that you can load when necessary.

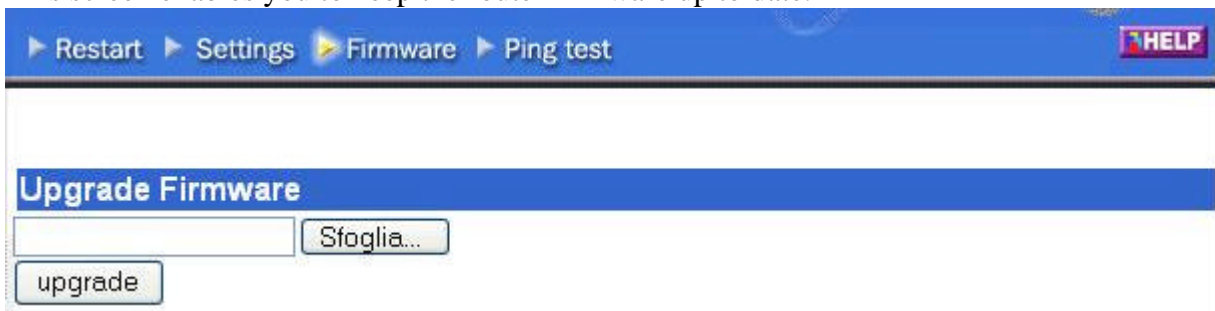
Load Settings: Click *Browse* and go to the location of a stored profile. Click *Load* to load the profile's settings.

Restore Factory Default Settings: Click to restore the default settings. All configuration changes you have made will be lost.

Setup Wizard: click to run a setup wizard that configures the router and interface

3.8.7.3 Firmware

This screen enables you to keep the router firmware up to date.



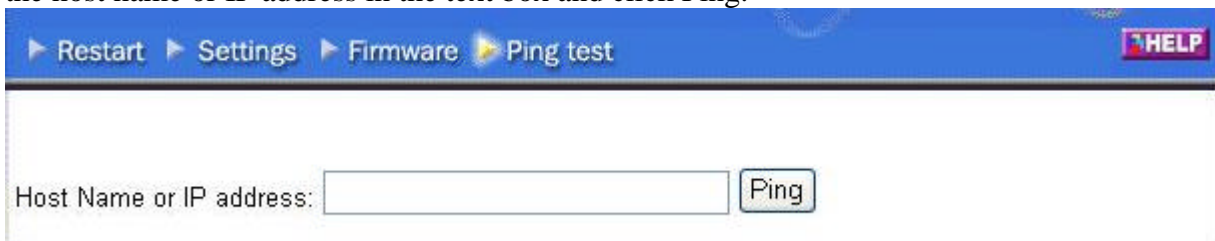
Please follow the below instructions:

1. Download the latest firmware from www.atlantis-land.com Web site, and save it to your disk.
2. Click *Browse* and go to the location of the downloaded firmware file.

Select the file and click Upgrade to update the firmware to the latest release

3.8.7.4 Ping Test

The ping test enables you to determine whether an IP address or host is present on the Internet. Type the host name or IP address in the text box and click Ping.



Quick Setup with Wizard

Setup wizard is provided as the part of the web configuration utility. You can simply follow the step-by-step process to get your wireless router configuration ready to run in 6 easy steps by clicking on the “**Wizard**” button on the function menu. The following screen will appear. Please click “**Next**” to continue.

>>>>> **Welcome to Wireless Router Setup Wizard**

Step 1. Set your new password
Step 2. Choose your time zone
Step 3. Set LAN connection and DHCP server
Step 4. Set internet connection
Step 5. Set wireless LAN connection
Step 6. Restart

display wizard next time? Yes No

Step 1: Set your new Password

You can change the password as you like and then click “**Next**” to continue.

>>>>> **Welcome to Wireless Router Setup Wizard**

Set Password

Password

Verify Password

Step2: Choose your time zone

Select your time zone from the drop down list. Please click “Next” to continue.

The screenshot shows the 'Choose Time Zone' step of the 'Welcome to Wireless Router Setup Wizard'. A dropdown menu is open, displaying '(GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna'. Below the dropdown are three buttons: '< Back', 'Next >', and 'Exit'.

Step 3: Set LAN connection and DHCP server

Set your IP address and mask. The default IP is 192.168.1.1. If you like to enable DHCP, please click “Enabled”. DHCP enabled is able to automatically assign IP addresses. Please assign the range of IP addresses in the fields of “Range start” and “Range end”. Please click “Next” to continue.

The screenshot shows the 'Set LAN & DHCP Server' step of the 'Welcome to Wireless Router Setup Wizard'. It contains several input fields and radio buttons:

LAN IP Address	192.168.1.1
LAN Subnet Mask	255.255.255.0
DHCP Server	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Range Start	192.168.1.100
Range End	192.168.1.199

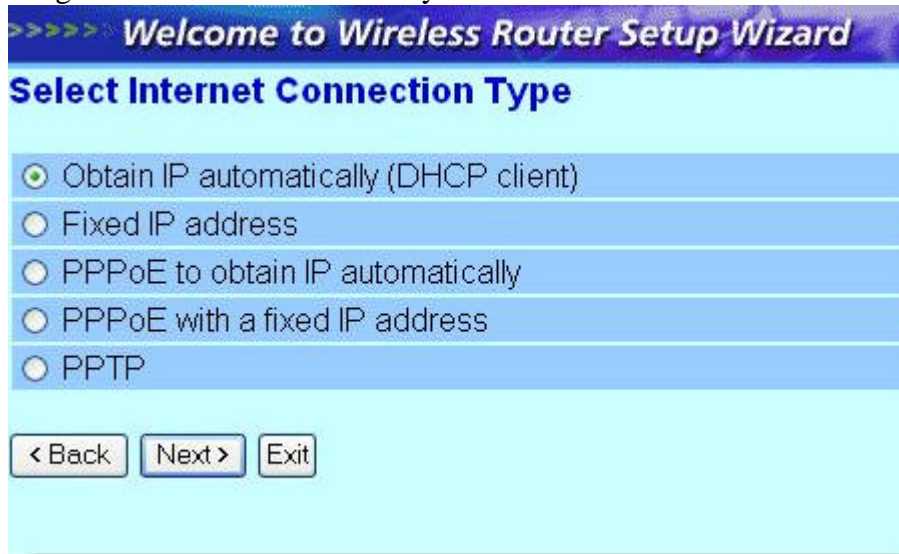
At the bottom, there are three buttons: '< Back', 'Next >', and 'Exit'.

Step 4: Set Internet connection

Select how the router will set up the Internet connection: Obtained IP automatically; Fixed IP address; PPPoE to obtain IP automatically; PPPoE with a fixed IP address; PPTP.

Obtain IP automatically (DHCP client):

If you have enabled DHCP server, choose "Obtain IP automatically (DHCP client)" to have the router assign IP addresses automatically.



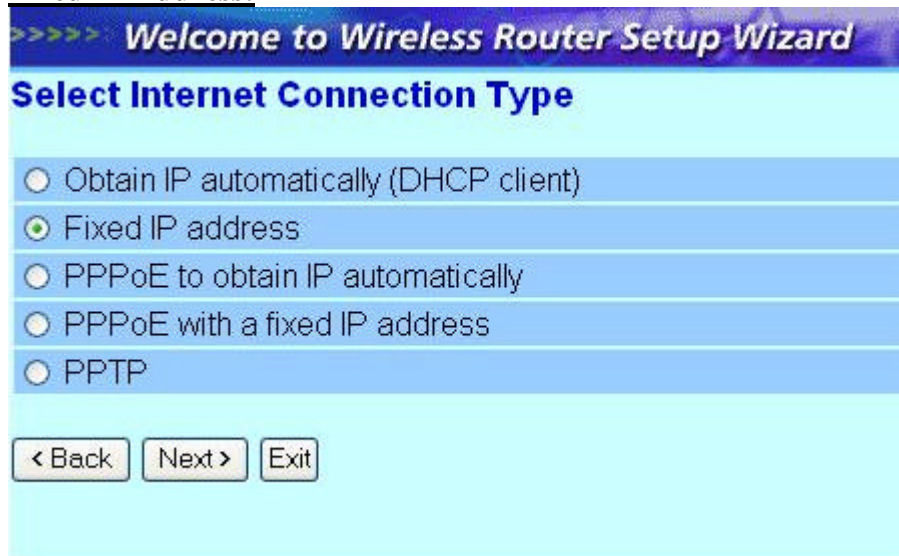
>>>> Welcome to Wireless Router Setup Wizard

Select Internet Connection Type

- Obtain IP automatically (DHCP client)
- Fixed IP address
- PPPoE to obtain IP automatically
- PPPoE with a fixed IP address
- PPTP

< Back Next > Exit

Fixed IP Address:



>>>> Welcome to Wireless Router Setup Wizard

Select Internet Connection Type

- Obtain IP automatically (DHCP client)
- Fixed IP address
- PPPoE to obtain IP automatically
- PPPoE with a fixed IP address
- PPTP

< Back Next > Exit

If Fixed IP address is assigned, the below screen will pop up. Please set the WAN address and DNS server.

>>>> Welcome to Wireless Router Setup Wizard

Set Fixed IP Address

WAN IP Address	<input type="text" value="0.0.0.0"/>
WAN Subnet Mask	<input type="text" value="0.0.0.0"/>
WAN Gateway Address	<input type="text" value="0.0.0.0"/>
DNS Server Address 1	<input type="text" value="0.0.0.0"/>
DNS Server Address 2	<input type="text" value="0.0.0.0"/>
DNS Server Address 3	<input type="text" value="0.0.0.0"/>

PPPoE to obtain IP automatically:

>>>> Welcome to Wireless Router Setup Wizard

Select Internet Connection Type

Obtain IP automatically (DHCP client)

Fixed IP address

PPPoE to obtain IP automatically

PPPoE with a fixed IP address

PPTP

>>>> Welcome to Wireless Router Setup Wizard

Set PPPoE to obtain IP automatically IP

User Name	<input type="text"/>
Password	<input type="password" value="....."/>
Verify Password	<input type="password" value="....."/>

PPPoE with a fixed IP address:

>>>>> Welcome to Wireless Router Setup Wizard

Select Internet Connection Type

- Obtain IP automatically (DHCP client)
- Fixed IP address
- PPPoE to obtain IP automatically
- PPPoE with a fixed IP address
- PPTP

>>>>> Welcome to Wireless Router Setup Wizard

Set PPPoe with a fixed IP Address

User Name	<input type="text"/>
Password	<input type="password"/>
Verify Password	<input type="password"/>
IP Address	<input type="text" value="0.0.0.0"/>

PPTP:

>>>>> Welcome to Wireless Router Setup Wizard

Select Internet Connection Type

Obtain IP automatically (DHCP client)

Fixed IP address

PPPoE to obtain IP automatically

PPPoE with a fixed IP address

PPTP

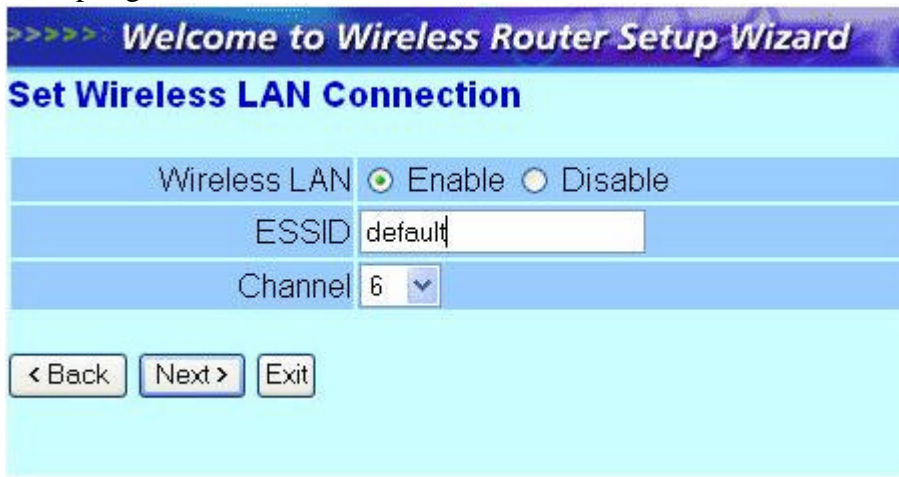
>>>>> Welcome to Wireless Router Setup Wizard

Set PPTP Client

My IP	<input type="text" value="0.0.0.0"/>
Subnet Mask	<input type="text" value="0.0.0.0"/>
GateWay	<input type="text" value="0.0.0.0"/>
Server IP	<input type="text" value="0.0.0.0"/>
PPTP Account	<input type="text"/>
PPTP Password	<input type="password"/>
Retype Password	<input type="password"/>

Step 5: Set Wireless LAN connection

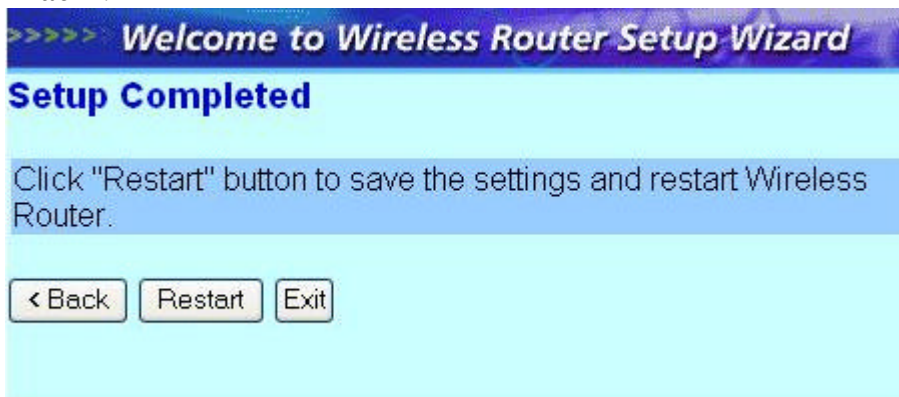
Click “enable” to enable wireless LAN. If you enable the wireless LAN, type the SSID in the text box and select a communications channel. The SSID and channel must be the same as wireless devices attempting communication to the router.



The screenshot shows the 'Set Wireless LAN Connection' screen of the 'Welcome to Wireless Router Setup Wizard'. The title bar reads '>>>> Welcome to Wireless Router Setup Wizard'. Below the title, the main heading is 'Set Wireless LAN Connection'. The form contains three rows: the first row has 'Wireless LAN' with 'Enable' selected (radio button) and 'Disable' unselected; the second row has 'ESSID' with a text box containing 'default'; the third row has 'Channel' with a dropdown menu showing '6'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Exit'.

Step 6: Restart

The Setup wizard is now completed. The new settings will be effective after the Wireless router restarted. Please click “**Restart**” to reboot the router. If you do not want to make any changes, please click “**exit**” to quit without any changes. You also can go back to modify the setting by clicking “**Back**”.



The screenshot shows the 'Setup Completed' screen of the 'Welcome to Wireless Router Setup Wizard'. The title bar reads '>>>> Welcome to Wireless Router Setup Wizard'. Below the title, the main heading is 'Setup Completed'. A message box contains the text: 'Click "Restart" button to save the settings and restart Wireless Router.'. At the bottom, there are three buttons: '< Back', 'Restart', and 'Exit'.

Technical Features

Physical Interfaces

WAN: 1 RJ45 10/100 Base-TX Fast Ethernet

LAN: 4 RJ45 10/100 Base-TX Fast Ethernet

Wireless 54Mbps (IEEE802.11g) and 11Mbps (IEEE802.11b)

8 Led for easy diagnostic and Reset

802.11b Interface

Chipset Atheros™ :AR2112(Radio)+AR2312

Dual antenna: Dipole External removable Antenna and Embedded Antenna

Radio Spec.

Standard IEEE802.11g and IEEE802.11b

DSSS(Direct Sequence Spread Spectrum)

Modulation: QPSK / BPSK / CCK and OFDM

Operating Channel: 13 (Europe), RF Frequency:2.400 GHz ~2.4835GHz

Data Rate (with automatic adaptation): 802.11g: Up to 54Mbps (with Automatic Fall-Back) and 108Mbps in SuperG™

Coverage Area: [Outdoor <100M ; Indoor <30M]

Advanced Characteristics

Atheros Super G™ capabilities to deliver 108 Mbps raw data rates and 90 Mbps TCP/IP throughput for 802.11g wireless LANs (Real-time hardware data compression, Dynamic transmit and modulation optimization and Standards-compliant bursting mode adapts to the network)

The chipsets fully support Wi-Fi Protected Access (WPA) and the IEEE 802.11i draft security standards in hardware and high-speed encryption engines for both the Temporal Key Integrity Protocol (TKIP) and the Advanced Encryption Standard (AES) with no performance degradation.

Security

Wi-Fi Protected Access (without performance degradation) and WEP 64/128

802.1x security (MD5 and TLS)

Port-Isolation (TBD), MAC Filtering and SSID Broadcast Disable function

Firewall Features:(Access- list control and rules, Stateful Packet Inspection (SPI), Domain Filtering (TBD), Packet Filtering, Ping of Death prevention, IP spoofing, Intrusion Detection, Security event log)

Standards & Protocols

Supports DHCP Server/Client, Static Router, PPOE and PPTP

UPnP support (TBD) and VPN pass through: L2TP, PPTP, IPSec

NAT/PAT, Virtual Server (10 entries) and Virtual DMZ host (1 entry)

Routing: RIPv1, RIPv2, TCP/IP v4, UDP, ICMP and SNMP MIPII (V1 and V3)

Configuration & Management

Web-based configuration utility

TFTP for software upgrade available, Status log and Network Timing Protocol (NTP)

Support Internet Application

ICQ, Netmeeting, MS messenger, PCanywhere, mIRC, CuSeeme...

Physical and Environmental

Power Consumption: (5V \pm 5%, 2.4A AC Adapter)

Dimensions/Weight : 205mm*115mm*35mm/ 350g

Temperature/Humidity: Operating:[0°C to 49°C], Storage:[-20°C to 65°C]: 5-95% (w/out condensing)

Package contents

I-Fly Wireless Broadband Router

CD-ROM containing drivers and the online manual (English, Italian and French)

Quick start guide (English and Italian), AC-DC power adapter and CAT-5 LAN cable

Glossary

Access Point

An interview networking device that seamlessly connects wired and wireless networks

Authentication

Authentication refers to the verification of a transmitted message's integrity.

DMZ

DMZ (DeMilitarized Zone) is a part of a network that is located between a secure LAN and an insecure WAN. DMZs provide a way for some clients to have unrestricted access to the Internet.

DHCP

DHCP (Dynamic Host Configuration Protocol) software automatically assigns IP addresses to client stations logging onto a TCP/IP network, which eliminates the need to manually assign permanent IP addresses.

DNS

DNS stands for Domain Name System. DNS converts machine names to the IP addresses that all machines on the net have. It translates from name to address and from address to name.

Domain Name

The domain name typically refers to an Internet site address.

DTIM

DTIM (Delivery Traffic Indication Message) provides client stations with information on the next opportunity to monitor for broadcast or multicast messages.

Filter

Filters are schemes which only allow specified data to be transmitted. For example, the router can filter specific IP addresses so that users cannot connect to those addresses.

Firewall

Firewalls are methods used to keep networks secure from malicious intruders and unauthorized access. Firewalls use filters to prevent unwanted packets from being transmitted. Firewalls are typically used to provide secure access to the Internet while keeping an organization's public Web server separate from the internal LAN.

Firmware

Firmware refers to memory chips that retain their content without electrical power (for example, BIOS ROM). The router firmware stores settings made in the interface.

Fragmentation

Refers to the breaking up of data packets during transmission.

FTP

FTP (File Transfer Protocol) is used to transfer files over a TCP/IP network, and is typically used for transferring large files or uploading the HTML pages for a Web site to the Web server.

Gateway

Gateways are computers that convert protocols enabling different networks, applications, and operating systems to exchange information.

Host Name

The name given to a computer or client station that acts as a source for information on the network.

HTTP

HTTP (HyperText Transport Protocol) is the communications protocol used to connect to servers on the World Wide Web. HTTP establishes a connection with a Web server and transmits HTML pages to client browser (for example Windows IE). HTTP addresses all begin with the prefix 'http://' prefix (for example, http://www.yahoo.com).

ICMP

ICMP (Internet Control Message Protocol) is a TCP/IP protocol used to send error and control messages over the LAN (for example, it is used by the router to notify a message sender that the destination node is not available).

IP

IP (Internet Protocol) is the protocol in the TCP/IP communications protocol suite that contains a network address and allows messages to be routed to a different network or subnet. However, IP does not ensure delivery of a complete message—TCP provides the function of ensuring delivery.

IP Address

The IP (Internet Protocol) address refers to the address of a computer attached to a TCP/IP network. Every client and server station must have a unique IP address. Clients are assigned either a permanent address or have one dynamically assigned to them via DHCP. IP addresses are written as four sets of numbers separated by periods (for example, 211.23.181.189).

ISP

An ISP is an organization providing Internet access service via modems, ISDN (Integrated Services Digital Network), and private lines.

LAN

LANs (Local Area Networks) are networks that serve users within specific geographical areas, such as in a company building. LANs are comprised of servers, workstations, a network operating system, and communications links such as the router.

MAC Address

A MAC address is a unique serial number burned into hardware adapters, giving the adapter a unique identification.

Metric

A number that indicates how long a packet takes to get to its destination.

MTU

MTU (Maximum Transmission/Transfer Unit) is the largest packet size that can be sent over a network. Messages larger than the MTU are divided into smaller packets.

NAT

NAT (Network Address Translation - also known as IP masquerading) enables an organization to present itself to the Internet with one address. NAT converts the address of each LAN node into one IP address for the Internet (and vice versa). NAT also provides a certain amount of security by acting as a firewall by keeping individual IP addresses hidden from the WAN.

(Network) Administrator

The network administrator is the person who manages the LAN within an organization. The administrator's job includes ensuring network security, keeping software, hardware, and firmware up-to-date, and keeping track of network activity.

NTP

NTP (Network Time Protocol) is used to synchronize the realtime clock in a computer. Internet primary and secondary servers synchronize to Coordinated Universal Time (UTC).

Packet

A packet is a portion of data that is transmitted in network communications. Packets are also sometimes called frames and datagrams. Packets contain not only data, but also the destination IP address.

Ping

Ping (Packet INternet Groper) is a utility used to find out if a particular IP address is present online, and is usually used by networks for debugging.

Port

Ports are the communications pathways in and out of computers and network devices (routers and switches). Most PCs have serial and parallel ports, which are external sockets for connecting devices such as printers, modems, and mice. All network adapters use ports to connect to the LAN. Ports are typically numbered.

PPPoE

PPPoE (Point-to-Point Protocol Over Ethernet) is used for running PPP protocol (normally used for dial-up Internet connections) over an Ethernet.

PPTP

Point-to-Point Tunneling Protocol uses TCP to deal data for tunnel maintenance, and uses PPP for sum up the information carried within the tunnel. The data carried within the tunnel can be compressed or encrypted. The encryption method used is RSA RC4. PPTP can operate when the protocol is supported only on the client and the server located on the other end that the client is corresponds with. No support is essential from any of the routers or servers within the network the two PCs are connecting across.

Protocol

A protocol is a rule that governs the communication of data.

RIP

RIP (Routing Information Protocol) is a routing protocol that is integrated in the TCP/IP protocol. RIP finds a route that is based on the smallest number of hops between the source of a packet and its destination.

RTS

RTS (Request To Send) is a signal sent from the transmitting station to the receiving station requesting permission to transmit data.

Server

Servers are typically powerful and fast machines that store programs and data. The programs and data are shared by client machines (workstations) on the network.

SMTP

SMTP (Simple Mail Transfer Protocol) is the standard Internet e-mail protocol. SMTP is a TCP/IP protocol defining message format and includes a message transfer agent that stores and forwards mail.

Subnet Mask

Subnet Masks (SUBNETwork masks) are used by IP protocol to direct messages into a specified network segment (i.e., subnet). A subnet mask is stored in the client machine, server or router and is compared with an incoming IP address to determine whether to accept or reject the packet.

SysLog Server

A SysLog server monitors incoming Syslog messages and decodes the messages for logging purposes.

TCP

(Transmission Control Protocol) is the transport protocol in TCP/IP that ensures messages over the network are transmitted accurately and completely.

TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) is the main Internet communications protocol. The TCP part ensures that data is completely sent and received at the other end. Another part of the TCP/IP protocol set is UDP, which is used to send data when accuracy and guaranteed packet delivery are not as important (for example, in real-time video and audio transmission). The IP component of TCP/IP provides data routability, meaning that data packets contain the destination station and network addresses, enabling TCP/IP messages to be sent to multiple networks within the LAN or in the WAN.

UDP

(User Datagram Protocol) is a protocol within TCP/IP that is used to transport information when accurate delivery isn't necessary (for example, real-time video and audio where packets can be dumped as there is no time for retransmitting the data).

Virtual Servers

Virtual servers are client servers (such as Web servers) that share resources with other virtual servers (i.e., it is not a dedicated server).

WAN

WAN (Wide Area Network) is a communications network that covers a wide geographic area such as a country (contrasted with a LAN, which covers a small area such as a company building).

Support

If you have any problems with the Wireless Router, please consult this manual.

If you continue to have problems you should contact the dealer where you bought this ADSL Router.

If you have any other questions you can contact the Atlantis Land company directly at the following address:

AtlantisLand spa

Via De Gasperi 122

20017 Mazzo di Rho(MI)

Tel: 02/93906085, 02/93907634(help desk)

Fax: 02/93906161

Email: info@atlantisland.it or tecnici@atlantisland.it

WWW: <http://www.atlantisland.it> or www.atlantis-land.com

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.